Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE DIRECT®

Journal of Complexity 19 (2003) 161–209

Journal of COMPLEXITY

http://www.elsevier.com/locate/jco

Systems of rational polynomial equations have polynomial size approximate zeros on the average ☆

D. Castro,[a] L.M. Pardo,[b,*] and J. San Martín[b]

[a] *Laboratoire GAGE, École Polytechnique, 91128 Palaiseau Cedex, France*

[b] *Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, E-39071 Santander, Spain*

Received 22 February 2002; revised 4 October 2002; accepted 17 October 2002

Abstract

A new technique for the geometry of numbers is exhibited. This technique provides sharp estimates on the number of bounded height rational points in subsets of projective space whose "projective cone" is semi-algebraic. This technique improves existing techniques as the one introduced by Davenport in (J. London Math. Soc. 26 (1951) 179). As main outcome, we conclude that systems of rational polynomial equations of bounded bit length have polynomial size approximate zeros on the average. We also conclude that the average number of projective real solutions of systems of rational polynomial equations of bounded bit length equals the square root of the Bézout number of the given system.

Keywords: Semi-algebraic sets; Probability and uniform distribution; Discrepancy bounds; Approximate zeros; Height of projective points

1. Introduction

A standard drawback for the running time of any algorithmic procedure is the output size of the procedure: lower bounds for the output length are also lower bounds for the running time. This technical idea has been systematically used to

☆ Research was partially supported by the Spanish grant BFM2000-0349.

*Corresponding author.

E-mail address: pardo@matesco.unican.es (L.M. Pardo).

0885-064X/03/$ - see front matter
doi:10.1016/S0885-064X(02)00028-6

establish lower complexity bounds for symbolic procedures that solve systems of multivariate polynomial equations (cf. [10,43,28,44] and the references therein).

In this paper, we deal with the output length of numerical analysis procedures that solve systems of multivariate polynomial equations. We follow Smale's approximate zero theory (cf. [5], Section 5 below and the references therein). An approximate zero of a system of polynomial equations F with associated zero ζ is a point z such that the sequence of iterates of the Newton operator of F is well defined and converges quadratically to ζ.

Within this theory, two are the main parameters that measure the output size:

(1) *The total number of solutions*. Also called the geometric degree of the solution variety (in the sense of [27]). In these pages, we restrict our discussion to real solutions. Hence we just want to know the total number of real solutions or, in a more topological language, the number of connected components (the 0th Betti number) of the solution variety.
(2) *The size of approximate zeros*. Namely, the number of tape cells in a Turing machine required to write down the list of digits describing the approximate zero. While binary (or decimal) encoding is used, this quantity is equivalent to the logarithmic height (in the sense of Weil) of the approximate zero (cf. also [25,32,33] and the references therein).

Both quantities are studied for input systems of multivariate polynomial equations with rational coefficients of bounded bit length. This restriction is quite natural and it was called the *computational hypothesis* in [12]. Roughly speaking, this computational hypothesis means that computing is discrete and not continuous. The standard theoretical model for computing is the well-established Turing machine model (or any equivalent one). Hence, when applying a numerical analysis procedure to an standard input, we know that the input, the intermediate results and the output are written over a finite alphabet. For instance, inputs should be systems of polynomial equations with coefficients in a discrete computational field (such as $\mathbb{Q}$) and outputs should be approximate zeros with coordinates in a discrete computational field ($\mathbb{Q}$ is again a good example for the real case). However, most theoretical models of numerical analysis procedures are *continuous* (see, for instance, the theoretical model discussed in [5]). Also studies on numerical analysis invariants (condition numbers, for instance) are based on the assumption that inputs belong to a continuous source space.

Hence there is a gap between standard studies of numerical analysis invariants and real life computing. These pages are an attempt to filling this gap with respect to quantities (i) and (ii) above.

For instance, there are easy-to-exhibit examples of systems of polynomial equations of bounded bit length such that the number of real solutions equals the *Bézout number* of the system (a quantity which is exponential in the number of variables).

In [11], three different techniques are introduced to exhibit lower bounds for the bit size of approximate zeros. Concrete examples of systems of multivariate

polynomial equations of small input length such that any approximate zero that satisfies Smale's γ-theorem requires exponential bit size are also shown in [11].

Under a continuous modelling, Shub and Smale have shown that the average number of real solutions of systems of polynomial equations with real coefficients equals the square root of the Bézout number (cf. [48] and Theorem 21 below). Observe that no estimate is discussed for the bit size of approximate zeros: under a continuous model the bit size of an approximate zero equals the number of coordinates.

The question to be answered in this paper is whether these average estimates for systems with real coefficients and real solutions can also be translated to the "discrete" case of systems with rational coefficients of bounded input length. The answer to this question needs of a transfer procedure from continuous to discrete estimates. This goes back to central problems in the geometry of numbers: *equidistribution*, *discrepancy bounds* (cf. [55,16,17,53], for instance). We introduce a new technique to obtain sharp discrepancy bounds based on the "syntactical description" of the considered set. Section 3 is devoted to state this new technique of the geometry of numbers which improves the method implicitly used in [12]. This technique may be resumed in the following statement.

Theorem 1. *Let $S\subseteq\mathbb{P}_m(\mathbb{R})$ be a subset of the projective space and assume $m\geqslant 2$. Let $\pi:\mathbb{R}^{m+1}\backslash\{0\}\to\mathbb{P}_m(\mathbb{R})$ be the canonical projection. Assume that $\tilde{S}:=\pi^{-1}(S)\cup\{0\}$ is a semi-algebraic set defined by a first-order formula involving only M existential quantifiers and at most s different polynomials of degree at most d.*

For every positive real number $h\in\mathbb{R}$, let $N(S,h)$ be the number of points $\underline{x}$ in $S\cap\mathbb{P}_m(\mathbb{Q})$ such that the (logarithmic) Weil's height of $\underline{x}$ is at most h.

Then, the following inequality holds:

$$\left|N(S,h)-\frac{Vol_{\mathbb{P}}(S)}{(m+1)\zeta(m+1)}2^{h(m+1)}\right|\leqslant\mathfrak{R}(S)2^{hm},$$

where $Vol_{\mathbb{P}}(S)$ is the projective volume of S in the Riemannian manifold $\mathbb{P}_m(\mathbb{R})$, ζ is Riemman's function and the constant $\mathfrak{R}(S)$ can be estimated in the following terms:

$$\mathfrak{R}(S)\leqslant(4(s+m)d+1)^{2(M+2)}6^{m+1}+\frac{Vol_{\mathbb{P}}(S)}{m+1}+\frac{1}{2}.$$

In the case that the cone $\tilde{S}$ is given by a quantifier free first-order formula, the upper bound for $\mathfrak{R}(S)$ is even sharper (cf. Theorem 14).

Once this technical tool has been stated, we are able to prove the following two main theorems:

Theorem 2. *The average number of real solutions of systems of rational polynomial equations of bounded bit length equals the square root of the Bézout number of the system.*

Theorem 3. *On the average, systems of homogeneous polynomial equations with rational coefficients of bounded bit length have polynomial size approximate zeros satisfying Smale's γ-theorem.*

Theorems 2 and 3 are immediate consequences of two more technical (but more precise) results (Theorems 4 and 5) that we state in Section 2 below.

The reader should observe that we are discussing input systems of bounded bit length (finite sets). Hence, we always assume a uniform probability distribution on finite sets. Observe that this uniform probability distribution also corresponds to the standard and natural practice of computing.

As we have used different notions coming from different fields and different approaches, and we want to make our pages as readable as possible, we have included most notions and most basic facts in separate Sections. So, Section 2 is devoted to introduce the basic notations required to state Theorems 4 and 5. Section 3 contains most basic facts about real algebraic geometry and the geometry of numbers used in these pages. In this Section, we proof Theorem 1. Section 4 is devoted to show Theorems 2 and 4. To this end we introduce some elimination theory and combine the continuous estimates obtained by Shub and Smale in [48] (cf. also Theorem 21) with the techniques and methods of the geometry of numbers introduced in Section 3 above. Finally, Section 5 is devoted to show Theorems 3 and 5. Once again, we combine the techniques and methods introduced in Section 3 with the average estimates for the condition number μ_{norm} in a continuous setting (cf. [48]). The main outcome of this section also improves the estimates obtained in [12].

2. Technical statements

This section is devoted to state in a precise form Theorems 2 and 3 above. In order to state these two outcomes we need to fix some preliminary notations.

For every positive integer number $d \in \mathbb{N}$, let $H_d^{\mathbb{Q}}$ be the rational vector space of all homogeneous polynomials with complex coefficients of degree d. Namely,

$$H_d^{\mathbb{Q}} := \{f \in \mathbb{Q}[X_0, \ldots, X_n] : f \text{ homogeneous, } \deg(f) = d\}.$$

For every list of degrees $(d) := (d_1, \ldots, d_n) \in \mathbb{N}^n$, let $\mathscr{H}_{(d)}^{\mathbb{Q}}$ be the rational vector space given by the following identity:

$$\mathscr{H}_{(d)}^{\mathbb{Q}} := H_{d_1}^{\mathbb{Q}} \times \cdots \times H_{d_n}^{\mathbb{Q}}.$$

For every list of degrees (d), we denote $D_{(d)}$ as $D_{(d)} := \max\{n, d_1, \ldots, d_n\}$ and by $\mathscr{D}_{(d)}$ we denote the Bézout number of (d). Namely,

$$\mathscr{D}_{(d)} := \prod_{i=1}^{n} d_i.$$

The space $\mathscr{H}_{(d)}^{\mathbb{Q}}$ is the space of systems of homogeneous polynomial equations with rational coefficients $F := [f_1, \ldots, f_n]$ such that for every i, $1 \leqslant i \leqslant n$, $\deg(f_i) = d_i$. For

every system $F \in \mathscr{H}_{(d)}^{\mathbb{Q}}$ we denote by $V_{\mathbb{C}}(F) \subseteq \mathbb{P}_n(\mathbb{C})$ the complex projective variety given by the following identity:

$$V_{\mathbb{C}}(F) \coloneqq \{\underline{x} \in \mathbb{P}_n(\mathbb{C}) : f_i(\underline{x}) = 0,\ 1 \leqslant i \leqslant n\}.$$

It is well-known that for a randomly chosen $F \in \mathscr{H}_{(d)}^{\mathbb{Q}}$ the set of common zeros $V_{\mathbb{C}}(F)$ is a zero-dimensional projective algebraic variety with high probability. Namely, $V_{\mathbb{C}}(F)$ is generically a non-empty finite set. If $V_{\mathbb{C}}(F)$ is a finite set, then the number of points in $V_{\mathbb{C}}(F)$ is at most the Bézout number $\mathscr{D}_{(d)}$. Moreover, for a randomly chosen $F \in \mathscr{H}_{(d)}^{\mathbb{Q}}$ the expected number of points in $V_{\mathbb{C}}(F)$ also equals the Bézout number $\mathscr{D}_{(d)}$.

This is no more true when we deal with real solutions of a system $F \in \mathscr{H}_{(d)}^{\mathbb{Q}}$. In order to study this difference, let $V_{\mathbb{R}}(F)$ be real algebraic set given by the following identity:

$$V_{\mathbb{R}}(F) \coloneqq V_{\mathbb{C}}(F) \cap \mathbb{P}_n(\mathbb{R}).$$

Examples of systems $F \in \mathscr{H}_{(d)}^{\mathbb{Q}}$ such that $V_{\mathbb{R}}(F)$ is a finite set and such that $\sharp(V_{\mathbb{R}}(F)) = \mathscr{D}_{(d)}$ are easy to obtain. However, this equality is not generically true.

We study the following two items:

(1) Sharp estimates for the probability that a randomly chosen system $F \in \mathscr{H}_{(d)}^{\mathbb{Q}}$ satisfies $V_{\mathbb{R}}(F)$ is a finite set.
(2) Sharp estimates for the average number of points in $V_{\mathbb{R}}(F)$.

As $V_{\mathbb{R}}(F)$ depends only on the linear subspace of $\mathscr{H}_{(d)}^{\mathbb{Q}}$ defined by F, we study both quantities for randomly chosen systems in the projective space $\mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$. For every non-negative integer number $k \in \mathbb{N}$, let $S_k \subseteq \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ be the set of all systems $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ such that $\sharp(V_{\mathbb{R}}(F)) = k$. Let $S_\infty \subseteq \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ be the set of all systems $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ such that $V_{\mathbb{R}}(F)$ is not a finite set.

As we are dealing with an infinite discrete projective space, we study these two types of sharp estimates as functions of the bit length of $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ (i.e. number of tape cells required to represent an input system F in a Turing machine). The bit length of F is essentially equivalent to the unitarily invariant logarithmic height of F (see Section 4.4 for a detailed definition).

For every positive real number $h > 0$, and for every $k \in \mathbb{N} \cup \{\infty\}$, let $S_k(h)$ be the set of all systems $F \in S_k$ of unitarily invariant bit length at most h. Similarly, let $\mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})(h)$ be the set of all systems $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ of unitarily invariant bit length at most h. Observe that both $S_k(h)$ and $\mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})(h)$ are finite sets.

We introduce the following additional notations. For every $k \in \mathbb{N} \cup \{\infty\}$ and for every $h > 0$, let $\mathscr{N}_{\Delta}(S_k, h)$ be the number of systems F in $S_k(h)$. Namely,

$$\mathscr{N}_{\Delta}(S_k, h) \coloneqq \sharp(S_k(h)).$$

Similarly, let $\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}}), h)$ be the number of systems F in $\mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})(h)$.

As $\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})(h)$ is a finite set, we assume it is endowed with the uniform probability distribution. Namely,

(1) The probability that a randomly chosen system $F \in \mathscr{H}^{\mathbb{Q}}_{(d)}(h)$ satisfies that $V_{\mathbb{R}}(F)$ is a finite set is given by

$$1 - \frac{\mathscr{N}_{\Delta}(S_{\infty}, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)}), h)}.$$

(2) The average number of points in $V_{\mathbb{R}}(F)$ for $F \in \mathscr{H}^{\mathbb{Q}}_{(d)}(h)$ is given by

$$\sum_{k=0}^{\infty} \frac{k\mathscr{N}_{\Delta}(S_k, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)}), h)}.$$

Let N be the (complex) dimension of the projective space $\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$. Observe that the following equality holds:

$$N = \left(\sum_{i=1}^{n} \binom{d_i + n}{n} \right) - 1.$$

These notations stated, Theorem 2 is an immediate consequence of the following more technical (but more complete statement).

Theorem 4. *With the same notations and assumptions as above, there is a universal constant C such that the following holds: Let $\epsilon > 0$ be a positive real number and let $h > 0$ be a positive real number such that the following inequality holds:*

$$h > 2(N + C)D_{(d)} \log D_{(d)} + 2(N + 1)\log(N + 1) - \log \epsilon.$$

Then, the following properties hold:

(1) *The probability that a randomly chosen system $F \in \mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ of bit length at most h satisfies $\sharp(V_{\mathbb{R}}(F)) < \infty$ is at least $1 - \epsilon$. Namely,*

$$1 - \frac{\mathscr{N}_{\Delta}(S_{\infty}, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)}), h)} \geqslant 1 - \epsilon.$$

(2) *The following inequality holds:*

$$\left| \sum_{k=0}^{\infty} \frac{k\mathscr{N}_{\Delta}(S_k, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)}), h)} - \sqrt{\mathscr{D}_{(d)}} \right| \leqslant \epsilon.$$

Similar arguments as those justifying the meaning of Theorem 4 can also be done to discuss the average size of approximate zeros of polynomial equations of bounded bit length. Using the techniques of Section 3, we improve the estimates of Theorem 4

of [12]. Then, we can obtain sharp estimates on the average size of approximate zeros. These sharp estimates are resumed in the following statement.

Theorem 5. *Let* $(d) \coloneqq (d_1, \ldots, d_n)$ *be a list of degrees and let* h, w *be two positive real numbers. Assume that the following inequality holds*:

$$h \geqslant \frac{N}{2}\log N + 18(n+2)^2(\log D_{(d)} + \log N) + 2(N+1) + \log w.$$

Then, for a randomly chosen system $F \in \mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ *of unitarily invariant bit length at most* h, *and for every* $\zeta \in V_{\mathbb{R}}(F)$, *there are approximate zeros* $x \in \mathbb{P}_n(\mathbb{Q})$ *of* F *with associated zero* ζ *of bit length at most*

$$2(n+2)^2[\log(D_{(d)}+1) + \log(n+1) + 5] + \frac{n}{4}\log w$$

with probability at least

$$1 - \frac{2}{w}.$$

Observe that Theorem 3 immediately follows from this Theorem 5.

The sequel is devoted to prove Theorems 1, 4 and 5.

3. Notions, notations and some geometry of numbers

This section is devoted to introduce some basic notions and notations and the proof of Theorem 1. Most of these notations are going to be used in the sequel. Here, we exhibit sharp estimates for the number of lattice points that belong to projective definable sets. These estimates are given in Proposition 10 and Theorems 14 and 15.

Both estimates are rather technical and require of some preliminary terminology. Thus, we postpone their statements to the corresponding subsections.

3.1. Notations for the projective space

The following constants are going to be used in the sequel. Let $\ell \in \mathbb{N}$ be a positive integer number. We denote by $K_\ell \in \mathbb{R}$ the volume of the ℓ-dimensional unit ball in $\mathbb{R}^\ell$. Namely,

$$K_\ell \coloneqq \frac{2\pi^{\frac{\ell}{2}}}{\ell\Gamma(\frac{\ell}{2})}. \tag{1}$$

For $\ell = 0$, we write $K_0 \coloneqq 1$. Finally, let us introduce the constant $\mathfrak{S}^{(m)}$ defined by

$$\mathfrak{S}^{(m)} \coloneqq \sum_{j=0}^{m-1} 3^{m-j-1}K_j. \tag{2}$$

For every positive integer number $m \in \mathbb{N}$, let $\mathbb{P}_m(\mathbb{R})$ be the real projective space of dimension m and let $\mathbb{P}_m(\mathbb{Q}) \coloneqq \mathbb{P}(\mathbb{Q}^{m+1})$ be the rational projective space of

dimension m. We denote by $\pi : \mathbb{R}^{m+1}\backslash\{0\} \to \mathbb{P}_m(\mathbb{R})$ the canonical projection onto the projective space. Namely, given $\underline{x} \coloneqq (x_0, \ldots, x_m) \in \mathbb{R}^{m+1}\backslash\{0\}$ we denote by $\pi(\underline{x}) \in \mathbb{P}_m(\mathbb{R})$ the projective point whose homogeneous coordinates are given by the following identity:

$$\pi(\underline{x}) \coloneqq (x_0 : x_1 : \ldots : x_m) \in \mathbb{P}_m(\mathbb{R}).$$

For every subset $S \subseteq \mathbb{P}_m(\mathbb{R})$, we define the *cone over* S as the subset $\tilde{S} \subseteq \mathbb{R}^{m+1}$ given by the following identity:

$$\tilde{S} \coloneqq \pi^{-1}(S) \cup \{0\}.$$

Let $\langle \cdot, \cdot \rangle : \mathbb{R}^{m+1} \times \mathbb{R}^{m+1} \to \mathbb{R}$ be the canonical Euclidean inner product in $\mathbb{R}^{m+1}$. For every $\underline{x} \in \mathbb{R}^{m+1}$, we denote its canonical Euclidean norm as $||\underline{x}|| \coloneqq (\langle \underline{x}, \underline{x} \rangle)^{1/2}$. For every real number $H > 0$, we denote by $B(0, H)$ the closed ball in $\mathbb{R}^{m+1}$ of radius H centred at the origin. Namely,

$$B(0, H) \coloneqq \{\underline{x} \in \mathbb{R}^{m+1} : ||\underline{x}|| \leqslant H\}.$$

This Euclidean inner product induces a natural Riemannian structure on $\mathbb{P}_m(\mathbb{R})$ which we denote by $(\mathbb{P}_m(\mathbb{R}), can)$. The distance induced by the Riemannian metric on $(\mathbb{P}_m(\mathbb{R}), can)$ is denoted by d_R. The Riemannian distance d_R is given by the following rule: given $\pi(\underline{x}), \pi(\underline{y}) \in \mathbb{P}_m(\mathbb{R})$, the Riemannian distance between $\pi(\underline{x})$ and $\pi(\underline{y})$ is given by the following identity:

$$d_R(\pi(\underline{x}), \pi(\underline{x}')) \coloneqq \arccos \frac{|\langle \underline{x}, \underline{x}' \rangle|}{||\underline{x}||||\underline{x}'||}.$$

We also introduce a projective distance $d_{\mathbb{P}}$ on $\mathbb{P}_m(\mathbb{R})$ from the previous Riemannian distance in the following terms: given $\pi(\underline{x}), \pi(\underline{x}') \in \mathbb{P}_m(\mathbb{R})$, the projective distance from $\pi(\underline{x})$ to $\pi(\underline{x}')$ is given by the following identity:

$$d_{\mathbb{P}}(\pi(\underline{x}), \pi(\underline{x}')) \coloneqq \sin d_R(\pi(\underline{x}), \pi(\underline{x}')).$$

Let S^m be the unit sphere in $\mathbb{R}^{m+1}$, namely

$$S^m \coloneqq \{\underline{x} \in \mathbb{R}^{m+1} : ||\underline{x}|| = 1\}.$$

The canonical Euclidean inner product in $\mathbb{R}^{m+1}$ also induces a Riemannian structure on S^m which we denote by (S^m, can). Let us also denote by $p_{\mathbb{R}} : S^m \to \mathbb{P}_m(\mathbb{R})$ the natural projection. Namely,

$$p_{\mathbb{R}} \coloneqq \pi|_{S^m}.$$

For every measurable subset $U \subseteq \mathbb{R}^{m+1}$ we denote by $Vol(U)$ the standard Lebesgue measure of U, i.e.

$$Vol(U) \coloneqq \int_{\mathbb{R}^{m+1}} \chi_U \, dx_0 \cdots dx_m,$$

where $\chi_U : \mathbb{R}^{m+1} \to \mathbb{R}$ is the characteristic function associated to U.

The canonical Riemannian structures on $\mathbb{P}_m(\mathbb{R})$ and S^m, respectively yield volume forms on each of those spaces. These volume forms lead to the following notions and notations.

For every measurable subset $U \subseteq S^m$ we define the spherical volume of U in the following terms:

$$Vol_S(U) := \int_{S^m} \chi_U(\theta)\, d\theta,$$

where $d\theta$ is the volume form in spherical coordinates and $\chi_U : S^m \to \mathbb{R}$ is the characteristic function associated to U. Observe that

$$Vol_S(S^m) = \frac{2\pi^{\frac{m+1}{2}}}{\Gamma(\frac{m+1}{2})},$$

where Γ is the gamma function.

Finally, for every measurable subset $U \subseteq \mathbb{P}_m(\mathbb{R})$, its projective volume satisfies:

$$Vol_{\mathbb{P}}(U) := \tfrac{1}{2}\, Vol_S(p_{\mathbb{R}}^{-1}(U)).$$

Let $\Delta \in GL(m+1, \mathbb{R})$ be a non-singular matrix. Let $\langle \cdot, \cdot \rangle_\Delta : \mathbb{R}^{m+1} \times \mathbb{R}^{m+1} \to \mathbb{R}$ be the inner product given by the following identity:

$$\langle \underline{x}, \underline{x'} \rangle_\Delta := \langle \Delta \underline{x}, \Delta \underline{x'} \rangle, \quad \forall \underline{x}, \underline{x'} \in \mathbb{R}^{m+1}.$$

For every $\underline{x} \in \mathbb{R}^{m+1}$, we denote by $||\underline{x}||_\Delta$ the norm of $\underline{x}$ with respect to this inner product. For every $H > 0$ we denote by $B_\Delta(0, H)$ the closed ball in $\mathbb{R}^{m+1}$ of radius H centred at the origin with respect to the norm $|| \cdot ||_\Delta$. Namely,

$$B_\Delta(0, H) := \{\underline{x} \in \mathbb{R}^{m+1} : ||\underline{x}||_\Delta \leqslant H\}.$$

The following equality holds for every $H > 0$ and every $\Delta \in GL(m+1, \mathbb{R})$:

$$\Delta(B_\Delta(0, H)) = B(0, H). \tag{3}$$

The inner product $\langle \cdot, \cdot \rangle_\Delta$ also induces a Riemannian structure in $\mathbb{P}_m(\mathbb{R})$ that we shall denote by $(\mathbb{P}_m(\mathbb{R}), \Delta)$. the following statement relates the Riemannian's structures $(\mathbb{P}_m(\mathbb{R}), can)$ and $(\mathbb{P}_m(\mathbb{R}), \Delta))$.

Lemma 6. *The following mapping is an isometry between* $(\mathbb{P}_m(\mathbb{R}), can)$ *and* $(\mathbb{P}_m(\mathbb{R}), \Delta)$:

$$\tilde{\Delta}^{-1} : (\mathbb{P}_m(\mathbb{R}), can) \to (\mathbb{P}_m(\mathbb{R}), \Delta),$$

where

$$\tilde{\Delta}^{-1}(x_0 : x_1 : \ldots : x_m) := \pi(\Delta^{-1}(x_0, x_1, \ldots, x_m))),$$

and $\Delta^{-1} \in GL(m+1, \mathbb{R})$ *is the inverse of the regular matrix* Δ.

Let $\tilde{\Delta}$ be the inverse of the isometry $\tilde{\Delta}^{-1}$ introduced above. Observe that for every $(x_0 : \ldots : x_m) \in \mathbb{P}_m(\mathbb{R})$ the following equality holds:

$$\tilde{\Delta}(x_0 : \ldots : x_m) = \pi(\Delta(x_0, \ldots, x_n)).$$

The inner product $\langle \cdot, \cdot \rangle_{\Delta}$ also induces a volume form in $\mathbb{P}_m(\mathbb{R})$. For every subset $U \subseteq \mathbb{P}_m(\mathbb{R})$ we denote by $Vol_{\Delta}(U)$ the volume of U with respect to the volume form induced by $\langle \cdot, \cdot \rangle_{\Delta}$. From Lemma 6 above the following holds for every subset $U \subseteq \mathbb{P}_m(\mathbb{R})$:

$$Vol_{\mathbb{P}}(\tilde{\Delta}(U)) = Vol_{\Delta}(U).$$

With the same arguments as in Corollary 33 of [12], we conclude the following statement:

Lemma 7. *Let $S \subseteq \mathbb{P}_m(\mathbb{R})$ be a subset of the projective space. For every $H > 0$, the following equalities hold*:

$$Vol(\tilde{S} \cap B_{\Delta}(0, H)) = \frac{2H^{m+1}}{(m+1)|\det(\Delta)|} Vol_{\Delta}(S),$$

$$Vol(\tilde{S} \cap B(0, H)) = \frac{2H^{m+1}}{(m+1)} Vol_{\mathbb{P}}(S).$$

3.2. Notations from real algebraic geometry

A *semi-algebraic set* is a subset W of some affine real space $\mathbb{R}^{m+1}$ that can be defined by a quantified first-order formula over the reals. A first-order formula $\Phi(X_1, \ldots, X_{m+1})$ that defines a semi-algebraic set $W \subseteq \mathbb{R}^{m+1}$ is also called a *syntactical description* of the semi-algebraic set W. A quantified first-order formula over the reals Φ is an expression that involves quantifiers $(\forall y_j \in \mathbb{R},\ \exists y_j \in \mathbb{R})$ and polynomial equations and inequalities. We say that a semi-algebraic set $W \subseteq \mathbb{R}^{m+1}$ is syntactically described by a family of s polynomials of degree at most d if there is a syntactical description Φ of W involving at most s different polynomials of total degree at most d.

From Tarski's Principle (cf. [51,46]) we know that every semi-algebraic set $W \subseteq \mathbb{R}^{m+1}$ has syntactical description given by quantifier free first-order formulae. Namely, a subset $W \subseteq \mathbb{R}^{m+1}$ is said to be semi-algebraic if there is a finite set of polynomials

$$\{f_{i,j}, g_{i,k} : 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s, 1 \leqslant k \leqslant t\} \subseteq \mathbb{R}[X_0, \ldots, X_m],$$

such that the following inequality holds:

$$W := \bigcup_{i=1}^{r} \{\underline{x} \in \mathbb{R}^{m+1} : f_{i,j}(\underline{x}) = 0, g_{i,k}(\underline{x}) > 0,\ 1 \leqslant j \leqslant s,\ 1 \leqslant k \leqslant t\}. \tag{4}$$

The term "semi-algebraic" is apparently due to Lojasiewicz (cf. [36]). We refer to [6] or [4] for additional information on semi-algebraic sets.

Now, we go deeper into the terminology in order to have simpler but precise statements in forthcoming Proposition 10 and Theorems 14 and 15.

Let $\mathscr{F} \coloneqq \{f_1, \ldots, f_s\} \subseteq \mathbb{R}[X_0, \ldots, X_m]$ be a finite set of polynomials. A semi-algebraic set $W \subseteq \mathbb{R}^{m+1}$ is called an *$\mathscr{F}$-cell* if there is a list of sign conditions

$$\underline{\epsilon} \coloneqq (\epsilon_1, \ldots, \epsilon_s) \in \{>, =, <\}^s,$$

such that

$$W \coloneqq \{\underline{x} \in \mathbb{R}^{m+1} : f_i(\underline{x})\epsilon_i \ 0, 1 \leqslant i \leqslant s\}.$$

An *$\mathscr{F}$-definable* semi-algebraic set is a finite union of $\mathscr{F}$-cells.

Definition 8. Let $s, d \in \mathbb{N}$ be two positive integer numbers. A semi-algebraic subset $W \subseteq \mathbb{R}^{m+1}$ is called (s, d)-definable if there is a finite set of polynomials $\mathscr{F} \subseteq \mathbb{R}[X_0, \ldots, X_m]$ satisfying:

(1) W is $\mathscr{F}$-definable,
(2) $\#(\mathscr{F}) = s$,
(3) $\deg(f) \leqslant d, \ \forall f \in \mathscr{F}$.

We say that a semi-algebraic subset $W \subseteq \mathbb{R}^{m+1}$ is the M-projection of an (s, d)-definable semi-algebraic set if there is an (s, d)-definable semi-algebraic subset $W' \subseteq \mathbb{R}^{M+m+1}$ such that the following equality holds:

$$W \coloneqq \{\underline{x} \in \mathbb{R}^{m+1} : \exists \underline{y} \in \mathbb{R}^M \text{ such that } (\underline{y}, \underline{x}) \in W'\}.$$

In other words, $W \subseteq \mathbb{R}^{m+1}$ is given by a quantified first-order formula such that

(1) The formula contains only existential quantifiers involving M additional variables (i.e. $\exists y_1 \in \mathbb{R}, \ldots, \exists y_M \in \mathbb{R}$).
(2) The formula involves at most s different polynomials (in the polynomial ring $\mathbb{R}[Y_1, \ldots, Y_M, X_1, \ldots, X_{m+1}]$) of total degree at most d.

A subset $S \subseteq \mathbb{P}_m(\mathbb{R})$ is said to have *semi-algebraic cone* if its cone $\tilde{S} \coloneqq \pi^{-1}(S) \cup \{0\} \subseteq \mathbb{R}^{m+1}$ is a semi-algebraic set.

For every subset $W \subseteq \mathbb{R}^{m+1}$, and for every non-negative integer $i \in \mathbb{N}$, let $\beta_i(W)$ be the ith Betti number. Recall that the 0th Betti number $\beta_0(W)$ of a subset $W \subseteq \mathbb{R}^{m+1}$ is the number of connected components of W.

In the mid 1960s, Milnor (cf. [38]), Thom (cf. [52]), Oleinik and Petrovsky (cf. [41,42]), and Warren (cf. [54]) exhibited upper bounds for the sum of Betti numbers of semi-algebraic sets in terms of their syntactical presentations. Now we recall some of their statements.

For a finite subset of polynomials $\mathscr{F} \subseteq \mathbb{R}[X_0, \ldots, X_m]$ of degree at most d, the number of non-empty $\mathscr{F}$-cells is bounded by a function that depends polynomially on $\sharp(\mathscr{F})$ and d, and that depends exponentially only on m. The proof of this fact may be seen in [54,27,39]. The following statement easily follows from these upper bounds for the number of non-empty $\mathscr{F}$-cells and the Milnor–Thom–Oleinik–Petrovsky upper bounds cited above:

Theorem 9. *Let $\mathscr{F} \coloneqq \{f_1, \ldots, f_s\} \subseteq \mathbb{R}[X_0, \ldots, X_m]$ be a finite set of polynomials of degree at most d. For every $\mathscr{F}$-definable semi-algebraic subset $W \subseteq \mathbb{R}^{m+1}$, the following inequality holds*:

$$\beta_0(W) \leqslant (2sd+1)^2 (4sd+1)^{2(m+1)}.$$

The bound in Theorem 9 is not optimal in the case $m = 1$ (i.e. when $W \subseteq \mathbb{R}$ is an $\mathscr{F}$-definable semi-algebraic set contained in the real line). In this particular case, one can easily get

$$\beta_0(W) \leqslant \#(\mathscr{F}) \max\{\deg f : f \in \mathscr{F}\} + 1. \tag{5}$$

3.3. Some geometry of numbers

In this subsection we show sharp estimates on the number of lattice points that belong to a given semi-algebraic subset $W \subseteq \mathbb{R}^{m+1}$.

We denote by $N(W)$ the number of points in W with integer coordinates. Namely,

$$N(W) \coloneqq \#(W \cap \mathbb{Z}^{m+1}).$$

It is well-known (cf. [40], for instance) that the following equality holds for compact semialgebraic sets $W \subseteq \mathbb{R}^{m+1}$:

$$\lim_{H \to \infty} \frac{N(HW)}{H^{m+1}} = Vol(W),$$

where $H \in \mathbb{R}$ is a positive real number and $HW \coloneqq \{Hx : x \in W\}$. Upper bounds for $|N(HW) - Vol(HW)|$ are usually called *discrepancy bounds* (cf. [16,17,53] and references therein for other approaches).

In [12] we used a sharp method due to Davenport (cf. [15]) to obtain discrepancy bounds for semi-algebraic sets in terms of their topological and intersection properties. In [12] we combined Davenport estimates with the upper bounds of the sum of Betti numbers of Milnor–Thom–Oleinik–Petrovsky (cf. Section 3.2 above) to find sharp discrepancy bounds in terms of the syntactical description of the given semi-algebraic set.

Here, we improve Davenport's estimates in Proposition 10 below. Davenport's original argument was a wise combination of induction and Fubini's Theorem. Here we add nothing essentially new to Davenport's proof: we also combine induction and Fubini's Theorem, but we combine these techniques in a sharper form in order to get better estimates.

During the Conference *FoCM'02*, Basu informed us that Koiran has also combined induction and Fubini's Theorem in [31] to give estimates on the number of points with integer coordinates in semi-algebraic sets.

Proposition 10. *Let $W \subseteq \mathbb{R}^{m+1}$ be an M-projection of an (s,d)-definable semi-algebraic set and let $H > 0$ be a positive real number. Let $N(W,H) \coloneqq N(W \cap B(0,H))$ be the number of points with integer coordinates in the intersection $W \cap B(0,H)$.*

Then, there is a constant $T(s,d,M,m+1)>0$ *(that only depends on* $m+1$ *and on the syntactical description of* W*) such that for every* $H>1$*, the following inequality holds*:

$$|N(W,H) - Vol(W\cap B(0,H))| \leqslant T(s,d,M,m+1)H^m, \tag{6}$$

where

$$T(s,d,M,m+1) \coloneqq (4d(s+m)+1)^{2(M+2)}\mathfrak{S}^{(m+1)},$$

and $\mathfrak{S}^{(m+1)}$ *is the constant introduced in Identity* (2).

For every $H,\ 0<H<1$*, the following also holds*:

$$|N(W,H) - Vol(W\cap B(0,H))| \leqslant T(s,d,m+1), \tag{7}$$

where $T(s,d,m+1) \coloneqq ((s+m)d+1)\mathfrak{S}^{(m+1)}$.

In particular, if $W\subseteq\mathbb{R}^{m+1}$ *is an* (s,d)*-definable semi-algebraic set, Inequality* (6) *can be replaced by*

$$|N(W,H) - Vol(W\cap B(0,H))| \leqslant T(s,d,m+1)H^m, \tag{8}$$

where $T(s,d,m+1) = ((s+m)d+1)\mathfrak{S}^{(m+1)}$.

Proof. We prove this proposition by induction on $n \coloneqq m+1$. For every $k\in\mathbb{N}$, $1\leqslant k\leqslant n$, and for every positive real number $H\in\mathbb{R}$, we denote by $B_k(0,H)\subseteq\mathbb{R}^k$ the closed ball in $\mathbb{R}^k$ of radius H centred at the origin. Our aim is to exhibit upper estimates for the following quantity:

$$\delta(W,n,H) \coloneqq \frac{1}{(2H+1)^n}\,|N(W,H) - Vol(W\cap B_n(0,H))|.$$

Let us introduce two auxiliary quantities to bound $\delta(W,n,H)$:

$$S_1 \coloneqq \frac{1}{(2H+1)^n}\left|N(W,H) - \sum_{x\in\mathbb{Z}\cap B_1(0,H)}\ \int_{\mathbb{R}^{n-1}}\chi_{W\cap B_n(0,H)}(x,y)\,dy\right|$$

and

$$S_2 \coloneqq \frac{1}{(2H+1)^n}\left|\sum_{x\in\mathbb{Z}\cap B_1(0,H)}\ \int_{\mathbb{R}^{n-1}}\chi_{W\cap B_n(0,H)}(x,y)\,dy - \ Vol(W\cap B_n(0,H))\right|.$$

We clearly have $\delta(W,n,H)\leqslant S_1+S_2$. Thus, we proceed by showing upper estimates for each term (S_1 and S_2) separately.

First of all, for every $x\in\mathbb{Z}\cap B_1(0,H)$, let $W_x\subseteq\mathbb{R}^{n-1}$ be the semi-algebraic subset given by the following identity:

$$W_x \coloneqq \{y\in\mathbb{R}^{n-1} : (x,y)\in W\cap B_n(0,H)\}.$$

Then, the following inequality follows from the definition of S_1:

$$S_1 \leqslant \frac{1}{(2H+1)^n}\sum_{x\in\mathbb{Z}\cap B_1(0,H)}|N(W_x,H) - Vol(W_x)|.$$

Finally, as $\#(\mathbb{Z}\cap B_1(0,H))=2H+1$, we conclude:

$$S_1\leqslant\frac{1}{(2H+1)^{n-1}}\max\{|N(W_x,H)-Vol(W_x)|:x\in\mathbb{Z}\cap B_1(0,H)\}.$$

As $d\geqslant 2$, and as $W\subseteq\mathbb{R}^n$ is the M-projection of an (s,d)-definable semi-algebraic set, then $W_x\subseteq\mathbb{R}^{n-1}$ is also the M-projection of an $(s+1,d)$-definable semi-algebraic set.

For every triple $s,d,n\in\mathbb{N}$ of positive numbers, let $\delta(s,d,M,n,H)$ be the maximum of the $\delta(V,n,H)$, where $V\subseteq\mathbb{R}^n$ is the M-projection of some (s,d)-definable semi-algebraic set. Our last inequality above also reads:

$$S_1\leqslant\delta(s+1,d,M,n-1,H). \tag{9}$$

As for S_2, by Fubini's theorem, we have

$$S_2\leqslant\frac{1}{(2H+1)^n}\times\int_{B_{n-1}(0,H)}\left|\sum_{x\in\mathbb{Z}\cap B_1(0,H)}\chi_{W\cap B_n(0,H)}(x,y)-\int_{B_1(0,H)}\chi_{W\cap B_n(0,H)}(x,y)\,dy\right|. \tag{10}$$

For every $y\in\mathbb{R}^{n-1}$, let $W^y\subseteq\mathbb{R}$ be the semi-algebraic set given by the following identity:

$$W^y:=\{x\in\mathbb{R}:(x,y)\in W\cap B_n(0,H)\}.$$

As $d\geqslant 2$, we may also conclude that $W^y\subseteq\mathbb{R}$ is the M-projection of an $(s+1,d)$-definable semi-algebraic set. From Davenport's estimates in [15] we have

$$\left|\sum_{x\in\mathbb{Z}}\chi_{W^y}(x)-\int_{\mathbb{R}}\chi_{W^y}(x)\,dx\right|\leqslant\beta_0(W^y), \tag{11}$$

where $\beta_0(W^y)$ is the number of connected components of W^y. Combining Inequalities (10) and (11), we conclude

$$S_2\leqslant\frac{K_{n-1}H^{n-1}}{(2H+1)^n}\max\{\beta_0(W^y):y\in\mathbb{R}^{n-1}\}.$$

From Theorem 9, we conclude the following inequality:

$$S_2\leqslant\frac{K_{n-1}H^{n-1}}{(2H+1)^n}(4(s+1)d+1)^{2(M+2)}. \tag{12}$$

Combining Inequalities (9) and (12) we conclude

$$\delta(W,n,H)\leqslant\delta(s+1,d,M,n-1,H)+\frac{K_{n-1}H^{n-1}}{(2H+1)^n}(4(s+1)d+1)^{2(M+2)}.$$

In other words, we have shown the following recurrence relation:

$$\delta(s,d,M,n,H)\leqslant\delta(s+1,d,M,n-1,H)+\frac{K_{n-1}H^{n-1}}{(2H+1)^n}(4(s+1)d+1)^{2(M+2)}. \tag{13}$$

From this recurrence relation, using Davenport's estimates for the case $n = 1$, we easily conclude

$$\delta(s,d,M,n,H) \leqslant (4(s+(n-1))d+1)^{2(M+2)} \left(\sum_{j=0}^{n-1} \frac{K_j H^j}{(2H+1)^{j+1}} \right).$$

Finally, noting that $|N(W,H) - Vol(W \cap B_n(0,H))| = (2H+1)^n \delta(W,n,H)$ and since $3H \geqslant 2H+1$ for $H \geqslant 1$, we conclude

$$|N(W,H) - Vol(W \cap B_n(0,H))| \leqslant (4(s+(n-1))d+1)\mathfrak{S}^{(n)} H^{n-1},$$

where $\mathfrak{S}^{(n)}$ is the constant introduced in Identity (2). This proves the first claim of the proposition.

As for the case $0 < H < 1$, Inequality (7) obviously follows from our arguments above.

In the case that $W \subseteq \mathbb{R}^n$ is an (s,d)-definable semi-algebraic set (i.e. in the particular case that W is the 0-projection of an (s,d)-definable semi-algebraic set) the previous estimates can be improved. This improvement follows the same steps of the first part of this proof until we arrive at Inequality (12). As W is an (s,d)-definable semi-algebraic set, $W^y \subseteq \mathbb{R}$ is also an $(s+1,d)$-definable semi-algebraic set. The bounds for $\beta_0(W^y)$ of Theorem 9 in the case $W^y \subseteq \mathbb{R}$ is $(s+1,d)$-definable, would yield:

$$S_2 \leqslant \frac{K_{n-1} H^{n-1}}{(2H+1)^n} ((s+1)d+1). \tag{14}$$

Then, combining Inequalities (9) and (14) we conclude the following recursion:

$$\delta(s,d,0,n,H) \leqslant \delta(s+1,d,0,n-1,H) + \frac{K_{n-1} H^{n-1}}{(2H+1)^n} ((s+1)d+1).$$

Applying this recursion instead of (13), we easily conclude that if $W \subseteq \mathbb{R}^{m+1}$ is an (s,d)-definable semi-algebraic set, the following holds:

$$|N(W,H) - Vol(W \cap B(0,H))| \leqslant ((s+(n-1))d+1)\mathfrak{S}^{(m+1)} H^m,$$

where $\mathfrak{S}^{(m+1)}$ is the constant introduced in Identity (2). □

A *lattice* Λ in $\mathbb{R}^{m+1}$ is the free Abelian group generated by a basis of $\mathbb{R}^{m+1}$ as real vector space. In particular, for every lattice $\Lambda \subseteq \mathbb{R}^{m+1}$, there is a non-singular matrix $A \in GL(m+1,\mathbb{R})$ such that

$$\Lambda = A\mathbb{Z}^{m+1} := \{A\underline{x} : \underline{x} \in \mathbb{Z}^{m+1}\}.$$

Such a matrix A is called *a generating matrix of the lattice* Λ.

Let $A, \Delta \in GL(m+1,\mathbb{R})$ be two regular matrices. Let $\Lambda := A\mathbb{Z}^{m+1}$ be the lattice generated by A. Let $W \subseteq \mathbb{R}^{m+1}$ be a subset and let $H \in \mathbb{R}$ be a positive real number. Let $N_\Delta(W,\Lambda,H)$ be the number of points in the intersection $W \cap \Lambda \cap B_\Delta(0,H)$, where $B_\Delta(0,H)$ is the closed ball of centre 0 and radius H defined by the norm $||\cdot||_\Delta : \mathbb{R}^{m+1} \to \mathbb{R}_+$ introduced in Section 3.

Observe that we have

$$A^{-1}(W \cap \Lambda \cap B_{\Delta}(0,H)) = (A^{-1}W \cap B_{\Delta A}(0,H)) \cap \mathbb{Z}^{m+1}.$$

Thus, we have

$$N_{\Delta}(W,\Lambda,H) = N(A^{-1}W \cap B_{\Delta A}(0,H)).$$

Observe that $B_{\Delta A}(0,H) \subseteq B(0, ||(\Delta A)^{-1}||_2 H)$, where $||(\Delta A)^{-1}||_2$ is the norm of the linear mapping defined by the regular matrix $(\Delta A)^{-1}$ with respect to the norm $||\cdot||_2$. The following statement is a consequence of Proposition 10.

Corollary 11. *Let $m \in \mathbb{N}$ be a positive integer number and assume $m \geqslant 2$. Let $A, \Delta \in GL(m+1,\mathbb{R})$ be two regular matrices. Let $\Lambda := A\mathbb{Z}^{m+1}$ be the lattice generated by A. Let $H \in \mathbb{R}$ be a positive real number and let $s,d \in \mathbb{N}$ be two positive integer numbers and assume $d \geqslant 2$. Let $W \subseteq \mathbb{R}^{m+1}$ be a semi-algebraic set. Then,*

(1) *If $W \subseteq \mathbb{R}^{m+1}$ is an (s,d)-definable semi-algebraic set, then the following inequalities hold:*

if $H||(\Delta A^{-1})||_2 \geqslant 1$, then

$$\left| N_{\Delta}(W,\Lambda,H) - \frac{Vol(W \cap B_{\Delta}(0,H))}{|\det(A)|} \right| \leqslant T(s,d,m+1)(||(\Delta A)^{-1}||_2)^m H^m,$$

else

$$\left| N_{\Delta}(W,\Lambda,H) - \frac{Vol(W \cap B_{\Delta}(0,H))}{|\det(A)|} \right| \leqslant T(s,d,m+1),$$

where $T(s,d,m+1)$ is the constant introduced in Proposition 10 above.

(2) *If $W \subseteq \mathbb{R}^{m+1}$ is the M-projection of an (s,d)-definable semi-algebraic set, then, the following holds:*

if $H||(\Delta A^{-1})||_2 \geqslant 1$, then

$$\left| N_{\Delta}(W,\Lambda,H) - \frac{Vol(W \cap B_{\Delta}(0,H))}{|\det(A)|} \right| \leqslant T(s,d,M,m+1)(||(\Delta A)^{-1}||_2)^m H^m,$$

else

$$\left| N_{\Delta}(W,\Lambda,H) - \frac{Vol(W \cap B_{\Delta}(0,H))}{|\det(A)|} \right| \leqslant T(s,d,M,m+1),$$

where $T(s,d,M,m+1)$ is the constant introduced in Proposition 10 above.

Let $\Lambda \subseteq \mathbb{R}^{m+1}$ be a lattice. A non-zero point $\underline{x} \in \Lambda \setminus \{0\}$ is said to be *visible from the origin* (or simply *visible*) if there is no point of Λ in the segment $[0,\underline{x}] \subseteq \mathbb{R}^{m+1}$ between the origin and $\underline{x}$.

Let $A \in GL(m+1,\mathbb{R})$ be the generating matrix of Λ, let $\underline{x} = (x_0,\ldots,x_m) \in \mathbb{Z}^{m+1}$ be a point with integer coordinates, and let $\underline{y} = A\underline{x} \in \Lambda$ be the corresponding point in the lattice Λ. Then, the point $\underline{y}$ is visible from the origin in Λ if and only if the greatest

common divisor of $\{x_0, \ldots, x_m\}$ is 1. Namely,

$$\underline{y} = A\underline{x} \quad \text{is visible if and only if} \quad \gcd(x_0, \ldots, x_m) = 1.$$

For every lattice $\Lambda \subseteq \mathbb{R}^{m+1}$ and for every non-zero real number $\rho \in \mathbb{R}\backslash\{0\}$, let $\Lambda(\rho)$ be the lattice given by the following identity:

$$\Lambda(\rho) \coloneqq \{\rho\underline{x} : \underline{x} \in \Lambda\}.$$

Visible points in a lattice Λ and projective points are closely related. We discuss here some of these relations.

Lemma 12. *Let $A, \Delta \in GL(m+1, \mathbb{R})$ be two regular matrices. Let $\Lambda \coloneqq A\mathbb{Z}^{m+1}$ be the lattice in $\mathbb{R}^{m+1}$ defined by A. Let $\underline{y} \in \Lambda$ be a point in the lattice. Then, $\underline{y}$ is a visible point if and only if the following equality holds*:

$$||\underline{y}||_\Delta = \min\{||\underline{z}||_\Delta : \underline{z} \in \Lambda,\ \pi(\underline{y}) = \pi(\underline{z})\},$$

where $||\cdot||_\Delta$ denotes the norm defined by Δ.

Let $\pi(\Lambda) \subseteq \mathbb{P}_m(\mathbb{R})$ be the projection of a lattice $\Lambda \coloneqq A\mathbb{Z}^{m+1}$. Observe that this projection verifies $\pi(\Lambda) = \tilde{A}\mathbb{P}_m(\mathbb{Q})$, where $\tilde{A} : \mathbb{P}_m(\mathbb{R}) \to \mathbb{P}_m(\mathbb{R})$ is the projective bijection defined by A. In the particular case $\Lambda = \mathbb{Z}^{m+1}(\rho)$, $\pi(\Lambda) = \mathbb{P}_m(\mathbb{Q})$ holds. Then, the following statement holds:

Lemma 13. *Let $S \subseteq \mathbb{P}_m(\mathbb{R})$ be a subset of the projective space $\mathbb{P}_m(\mathbb{R})$ and let $\Lambda \subseteq \mathbb{R}^{m+1}$ be a lattice. Then, the number of visible points in $\tilde{S} \cap \Lambda$ is two times the number of projective points in $S \cap \pi(\Lambda)$.*

Given a subset $S \subseteq \mathbb{P}_m(\mathbb{R})$ with semi-algebraic cone $\tilde{S} \subseteq \mathbb{R}^{m+1}$ and given a lattice Λ we want to have estimates for the number of points in the intersection $S \cap \pi(\Lambda)$. This is achieved in the following two theorems:

Theorem 14. *Let $A, \Delta \in GL(m+1, \mathbb{R})$ be two regular matrices. Let $\Lambda \coloneqq A\mathbb{Z}^{m+1}$ be the lattice generated by A. Let $s, d \in \mathbb{N}$ be two positive integers and assume that $d \geqslant 2$. Let $S \subseteq \mathbb{P}_m(\mathbb{R})$ be a subset of the projective space such that its cone $\tilde{S} \subseteq \mathbb{R}^{m+1}$ is an (s, d)-definable semi-algebraic set. Let $H \in \mathbb{R}$ be a positive real number. Assume that $H \geqslant 1$ and $m \geqslant 2$.*

Let $\mathcal{N}_\Delta(S, \Lambda, H)$ be the number of projective points in $S \cap \pi(\Lambda \cap B_\Delta(0, H))$. Namely,

$$\mathcal{N}_\Delta(S, \Lambda, H) \coloneqq \sharp(S \cap \pi(\Lambda \cap B_\Delta(0, H))).$$

Then, the following inequality holds:

$$|\mathcal{N}_\Delta(S, \Lambda, H) - \mathcal{V}_\Delta(S, \Lambda)H^{m+1}| \leqslant \mathfrak{R}_\Delta(S, \Lambda)H^m,$$

where

$$\mathscr{V}_{\Delta}(S,\Lambda) \coloneqq \frac{Vol_{\Delta}(S)}{(m+1)|\det(\Delta A)|\zeta(m+1)},$$

$$\mathfrak{R}_{\Delta}(S,\Lambda) \coloneqq T(s,d,m+1)||(\Delta A)^{-1}||_2^m + \frac{Vol_{\Delta}(S)}{(m+1)|\det(\Delta A)|\,||(\Delta A)^{-1}||_2} + \frac{||(\Delta A)^{-1}||_2}{2}, \tag{15}$$

ζ is Riemmann's function and $T(s,d,m+1)$ is the constant introduced in Proposition 10.

We also have the following statement for M-projections of (s,d)-definable semi-algebraic sets.

Theorem 15. *Let m, A, Δ, Λ, H be as in the theorem above. Let $S \subseteq \mathbb{P}_m(\mathbb{R})$ be a subset of the projective space and assume that its cone $\tilde{S} \subseteq \mathbb{R}^{m+1}$ is the M-projection of an (s,d)-definable semi-algebraic set. Let $\mathscr{N}_{\Delta}(S,\Lambda,H)$ be the number of projective points in the intersection $S \cap \pi(\Lambda \cap B_{\Delta}(0,H))$. Then, the following inequality holds*:

$$|\mathscr{N}_{\Delta}(S,\Lambda,H) - \mathscr{V}_{\Delta}(S,\Lambda)H^{m+1}| \leqslant \mathfrak{R}_{\Delta}^{(M)}(S,\Lambda)H^m,$$

where $\mathscr{V}_{\Delta}(S,\Lambda)$ is the constant introduced in Theorem 14,

$$\mathfrak{R}_{\Delta}^{(M)}(S,\Lambda) \coloneqq T(s,d,M,m+1)||(\Delta A)^{-1}||_2^m + \frac{Vol_{\Delta}(S)}{(m+1)|\det(\Delta A)|||(\Delta A)^{-1}||_2} + \frac{||(\Delta A)^{-1}||_2}{2}, \tag{16}$$

and $T(s,d,M,m+1)$ is the constant introduced in Proposition 10 *above*.

Both theorems have a similar proof. The only difference consists in replacing Inequality (6) by Inequality (8) in Proposition 10. Hence, we just include the Proof of Theorem 14.

Proof of Theorem 14. Let $V \subseteq \mathbb{R}^{m+1}$ be the bounded semi-algebraic subset given by the following identity:

$$V \coloneqq B_{\Delta A}(0,1) \bigcap A^{-1}\tilde{S}.$$

As $\tilde{S}$ is a cone, we easily conclude that for every positive real number $H \in \mathbb{R}_+$,

$$HV = B_{\Delta A}(0,H) \bigcap A^{-1}\tilde{S}.$$

In particular, for every positive real number $H \in \mathbb{R}_+$ we have

$$H^{m+1}\,Vol(V) = Vol(A^{-1}\tilde{S} \cap B_{\Delta A}(0,H)) = \frac{Vol(\tilde{S} \cap B_{\Delta}(0,H))}{|\det(A)|}. \tag{17}$$

Next, observe that for every positive number $H \in \mathbb{R}_+$ the following equality holds:

$$A^{-1}(\tilde{S} \cap \Lambda \cap B_\Delta(0,H)) = (A^{-1}\tilde{S} \cap B_{\Delta A}(0,H)) \cap \mathbb{Z}^{m+1} = (HV) \cap \mathbb{Z}^{m+1}.$$

Moreover, A^{-1} identifies the visible points of Λ in $\tilde{S} \cap B_\Delta(0,H)$ with the visible points of $\mathbb{Z}^{m+1}$ in $HV \subseteq \mathbb{R}^{m+1}$. From Lemma 13 we conclude:

$$\mathcal{N}_\Delta(\tilde{S}, \Lambda, H) = \frac{1}{2}\mathcal{N}(HV),$$

where

$$\mathcal{N}(HV) = \sharp\{\underline{x} \in \mathbb{Z}^{m+1} \cap (HV) : \underline{x} \text{ is visible in } \mathbb{Z}^{m+1}\}.$$

Hence, we estimate $\mathcal{N}(A^{-1}\tilde{S} \cap B_{\Delta A}(0,H))$ by an argument which is largely inspired by the Proof of Theorem 459 of [26] and the methods discussed in [12].

For every positive real number $\rho \in \mathbb{R}_+$, let us denote by A_ρ the finite subset of $B_{\Delta A}(0,1)$ given by the following equality:

$$A_\rho := V \cap \mathbb{Z}^{m+1}(\rho) \backslash \{0\}.$$

Let $g(\rho)$ be the number of points in A_ρ. As $\tilde{S}$ is a cone, the following equality holds:

$$g(\rho) = \sharp(A^{-1}\tilde{S} \cap B_{\Delta A}(0,\rho^{-1}) \cap \mathbb{Z}^{m+1}) - 1 = N_\Delta(\tilde{S}, \Lambda, \rho^{-1}) - 1. \tag{18}$$

Let $f(\rho)$ be the number of points in A_ρ which are visible from the origin. Observe that the following holds:

$$f(\rho) = \mathcal{N}(A^{-1}\tilde{S} \cap B_{\Delta A}(0,\rho^{-1})) = \mathcal{N}(\rho^{-1}V).$$

As in the Proof of Theorem 459 of [26] we may easily conclude that

$$g(\rho) = \sum_{n=1}^{\infty} f(n\rho).$$

From Möbius inversion formula (see Theorem 270 in [26], for instance) it follows that

$$f(\rho) = \sum_{n=1}^{\infty} \mu(n) g(n\rho),$$

where μ is Möbius function. Observe that Riemann's ζ function satisfies the following identity for every $s > 1$ (cf. [26, Theorem 287], for instance):

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}. \tag{19}$$

Hence, we have

$$\rho^{m+1} f(\rho) - \frac{Vol(V)}{\zeta(m+1)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{m+1}} ((n\rho)^{m+1} g(n\rho) - Vol(V)). \tag{20}$$

Let $\mathbb{N}_\rho$ be the set of positive integer numbers given by the following identity:

$$\mathbb{N}_\rho := \{n \in \mathbb{N} : 1 \leqslant n \leqslant \rho^{-1} ||(\Delta A)^{-1}||_2\}.$$

Let $\mathbb{N}'_\rho := \mathbb{N}\backslash\mathbb{N}_\rho$ be the set of positive integer numbers given by the following identity:

$$\mathbb{N}'_\rho := \{n\in\mathbb{N};\ : n\rho > ||(\Delta A)^{-1}||_2\}.$$

Observe that for every $n\in\mathbb{N}'_\rho$, $A_{n\rho}=\emptyset$ and $g(n\rho)=0$. For if $n\in\mathbb{N}'_\rho$ and $x\in A_{n\rho}$, then $x\in\mathbb{Z}^{m+1}(n\rho)\backslash\{0\}$ and $x\in B_{\Delta A}(0,1)$. Then, there is a non-zero point with integer coordinates $y\in\mathbb{Z}^{m+1}$ such that $x=(n\rho)y$. Hence, the following chain of inequalities hold:

$$1\geqslant||(\Delta A)x||_2=(n\rho)||(\Delta A)y||_2\geqslant(n\rho)\frac{||y||_2}{||(\Delta A)^{-1}||_2}.$$

As $y\neq0$ and $y\in\mathbb{Z}^{m+1}$, then $||y||_2\geqslant1$ and we should obtain $1\geqslant||(\Delta A)x||_2>1$. Thus, we may rewrite Eq. (20) as

$$\rho^{m+1}f(\rho)-\frac{Vol(V)}{\zeta(m+1)}=\Sigma_\rho+\Sigma'_\rho,$$

where

$$\Sigma_\rho := \sum_{n\in\mathbb{N}_\rho}\frac{\mu(n)}{n^{m+1}}((n\rho)^{m+1}g(n\rho)-Vol(V))$$

and

$$\Sigma'_\rho := -\sum_{n\in\mathbb{N}'_\rho}\frac{\mu(n)}{n^{m+1}}Vol(V).$$

Now, assume that $n\in\mathbb{N}_\rho$ (i.e. $(n\rho)^{-1}||(\Delta A)^{-1}||_2\geqslant1$). Then, replacing $(n\rho)^{-1}$ by H, we conclude from Identities (17) and (18) above the following identity:

$$|(n\rho)^{m+1}g(n\rho)-Vol(V)|=\frac{|N_\Delta(\tilde{S},\Lambda,H)-(1+Vol(HV))|}{H^{m+1}}. \tag{21}$$

From the first Claim of Corollary 11 above, we have

$$\frac{1}{H^{m+1}}|N_\Delta(\tilde{S},\Lambda,H)-Vol(HV)|\leqslant\frac{T(s,d,m+1)||(\Delta A)^{-1}||_2^m}{H},$$

where $T(s,d,m+1)$ is the constant introduced in Proposition 10 above.

Replacing back H by $(n\rho)^{-1}$, Eq. (21) becomes the following inequality:

$$|(n\rho)^{m+1}g(n\rho)-Vol(V)|\leqslant T(s,d,m)\mathfrak{S}^{(m+1)}||(\Delta A)^{-1}||_2^m n\rho+(n\rho)^{m+1}. \tag{22}$$

We conclude

$$|\Sigma_\rho|\leqslant\sum_{n\in\mathbb{N}_\rho}\left(\frac{1}{n^m}\rho T(s,d,m)\mathfrak{S}^{(m+1)}||(\Delta A)^{-1}||_2^m\right)+\sum_{n\in\mathbb{N}_\rho}\rho^{m+1}. \tag{23}$$

Then, we conclude

$$|\Sigma_\rho|\leqslant\rho\zeta(m)T(s,d,m)\mathfrak{S}^{(m+1)}||(\Delta A)^{-1}||_2^m+||(\Delta A)^{-1}||_2\rho^m. \tag{24}$$

On the other hand, the following inequality holds:

$$|\Sigma'_\rho| \leqslant \left(\sum_{n > \rho^{-1}||(\Delta A)^{-1}||_2} \frac{1}{n^{m+1}} \right) Vol(V) \leqslant \frac{\rho\, Vol(V)}{||(\Delta A)^{-1}||_2}. \tag{25}$$

Finally, combining Eqs. (24), (25), and noting that $\zeta(m) \leqslant \zeta(2) = \frac{\pi^2}{6}$, we conclude

$$\left| \rho^{m+1} f(\rho) - \frac{Vol(V)}{\zeta(m+1)} \right| \leqslant \rho \left[2T(s,d,m+1)||(\Delta A)^{-1}||_2^m + \frac{Vol(V)}{||(\Delta A)^{-1}||_2} + ||(\Delta A)^{-1}||_2 \rho^{m-1} \right]. \tag{26}$$

Finally, replacing ρ^{-1} by H in this equation and using the identity described in Eq. (17) we conclude

$$\left| f(H^{-1}) - \frac{Vol(\tilde{S} \cap B_\Delta(0,1))}{|\det(A)|\zeta(m+1)} H^{m+1} \right| \leqslant H^m \left[2T(s,d,m+1)||(\Delta A)^{-1}||^m + \frac{Vol(\tilde{S} \cap B_\Delta(0,1))}{|\det(A)|\, ||(\Delta A)^{-1}||_2} \right] + H||(\Delta A)^{-1}||_2. \tag{27}$$

And the statement follows noting that $\mathcal{N}_\Delta(S, \Lambda, H) = 1/2f(H^{-1})$. □

Remark 16. The previous theorem holds for $m \geqslant 2$. For the case $m = 1$, a slightly different estimate may be found, provided that

$$H > \max\left\{ 1, \frac{1}{||(\Delta A)^{-1}||_2} \right\}.$$

In this case, the following inequality holds:

$$|\mathcal{N}_\Delta(S, \Lambda, H) - \mathcal{V}_\Delta(S, \Lambda) H^2| \leqslant \mathfrak{R}_\Delta(S, \Lambda) H \log(H),$$

where

$$\mathcal{V}_\Delta(S, \Lambda) := \frac{Vol_\Delta(S)}{2|\det(\Delta A)|\zeta(2)},$$

$$\mathfrak{R}_\Delta(S, \Lambda) := T(s,d,2)||(\Delta A)^{-1}|| + \frac{Vol_\Delta(S)}{2|\det(\Delta A)|||(\Delta A)^{-1}||_2} + \frac{||(\Delta A)^{-1}||_2}{2},$$

and $T(s,d,2)$ is the constant introduced in Corollary 11. The reader may obtain this estimate by the same arguments as those used in the Proof of the previous theorem.

Let us now introduce the *Northcott–Schmidt height* of a projective point. Let $\mathcal{P} \subseteq \mathbb{N}$ be the class of all prime numbers. For every $p \in \mathcal{P}$, let $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ be the non-archimedean p-adic absolute value.

Definition 17. Let $\Lambda \subseteq \mathbb{R}^{m+1}$ be a lattice generated by the regular matrix $A \in GL(m+1,\mathbb{R})$. Let $y \coloneqq \tilde{A}x \in \pi(\Lambda)$ be a projective point in the lattice such that $x \coloneqq (x_0 : \ldots : x_m) \in \mathbb{P}_m(\mathbb{Q})$. We define the Northcott–Schmidt height of the projective point y in $\pi(\Lambda)$ in the following terms:

$$H(y) \coloneqq ||\underline{x}||_2 \prod_{p \in \mathscr{P}} \max\{|x_i|_p : 0 \leqslant i \leqslant m\}.$$

We define the logarithmic height of y as $ht(y) \coloneqq \log H(y)$.

This notion is well-defined because of *Weil's product formula*. Observe that the logarithmic height of $y \coloneqq \tilde{A}(x)$, where $x \in \mathbb{P}_m(\mathbb{Q})$ is essentially, the number of tape cells in a Turing machine required to represent the projective point x. It is also the number of tape cells required to represent y in a Turing machine, provided that A is fixed and given 'a priori'. Within a computer science context, the logarithmic height of y is also called the *bit length* of y (provided that A is fixed).

Corollary 18. *Let $A \in GL(m+1,\mathbb{R})$ be a regular matrix and let $\Lambda \coloneqq A\mathbb{Z}^{m+1}$ be the lattice generated by A. Let $S \subseteq \mathbb{P}_m(\mathbb{R})$ be a subset of the projective space whose cone $\tilde{S} \subseteq \mathbb{R}^{m+1}$ is a semi-algebraic set. Assume $m \geqslant 2$ and let $\mathscr{N}(S,\Lambda,h)$ be the number of projective points in $S \cap \pi(\Lambda)$ of bit length at most h. Then, there is a constant $\mathfrak{R}(S,\Lambda)$ such that the following inequality holds*:

$$|\mathscr{N}(S,\Lambda,h) - \mathscr{V}(S,\Lambda)2^{h(m+1)}| \leqslant \mathfrak{R}(S,\Lambda)2^{hm},$$

where

$$\mathscr{V}(S,\Lambda) \coloneqq \frac{Vol_{\mathbb{P}}(\tilde{A}^{-1}S)}{(m+1)\zeta(m+1)}.$$

The constant $\mathfrak{R}(S,\Lambda)$ can be estimated from syntactical descriptions of S and from the matrix A in the following terms:

(1) *if the cone $\tilde{S} \subseteq \mathbb{R}^{m+1}$ is an (s,d)-definable semi-algebraic set, we have*

$$\mathfrak{R}(S,\Lambda) \leqslant T(s,d,m+1) + \frac{Vol_{\mathbb{P}}(\tilde{A}^{-1}S)}{(m+1)} + \frac{1}{2},$$

where $T(s,d,m+1)$ is the constant introduced in Proposition 10.

(2) *if the cone $\tilde{S} \subseteq \mathbb{R}^{m+1}$ is the M-projection of an (s,d)-definable semi-algebraic set, we have*

$$\mathfrak{R}(S,\Lambda) \leqslant T(s,d,M,m+1) + \frac{Vol_{\mathbb{P}}(\tilde{A}^{-1}S)}{(m+1)} + \frac{1}{2},$$

where $T(s,d,M,m+1)$ is the constant introduced in Proposition 10.

Proof. We just make the proof of the first claim. Observe that the number $\mathscr{N}(S,\Lambda,h)$ is one half of the number of visible points $y \coloneqq Ax$ in Λ that belong to $\tilde{S}$

and such that the following inequality holds:

$$||x||_2 := ||A^{-1}y||_2 = ||y||_{A^{-1}} \leqslant 2^h.$$

Hence,

$$\mathscr{N}(S, \Lambda, h) = \mathscr{N}_{A^{-1}}(S, \Lambda, 2^h).$$

Then, applying Theorem 14 we conclude

$$|\mathscr{N}(S, \Lambda, h) - \mathscr{V}(S, \Lambda)2^{h(m+1)}| \leqslant \mathfrak{R}(S, \Lambda)2^{hm}.$$

where

$$\mathscr{V}(S, \Lambda) := \frac{Vol_{\mathbb{P}}(\tilde{A}^{-1}S)}{(m+1)\zeta(m+1)},$$

$$\mathfrak{R}(S, \Lambda) := T(s, d, m+1) + \frac{Vol_{\mathbb{P}}(\tilde{A}^{-1}S)}{m+1} + \frac{1}{2},$$

and $T(s, d, m+1)$ is the constant introduced in Corollary 10. □

4. Average number of real solutions of systems of homogeneous polynomial equations with rational coefficients

4.1. Two Riemannian structures in $\mathscr{H}^{\mathbb{R}}_{(d)}$

Notations are mainly those of [5]. We define $H^{\mathbb{R}}_d$ as the set of all real homogeneous polynomials in $n+1$ variables of degree d. Namely,

$$H^{\mathbb{R}}_d := \{f \in \mathbb{R}[X_0, \ldots, X_n] : f \text{ homogeneous, } \deg(f) = d\}.$$

We denote by $H^{\mathbb{Q}}_d$ the set of all homogeneous polynomial $f \in H^{\mathbb{R}}_d$ with rational coefficients. Namely,

$$H^{\mathbb{Q}}_d := H^{\mathbb{R}}_d \cap \mathbb{Q}[X_0, \ldots, X_n].$$

We define the standard Euclidean inner product in $H^{\mathbb{R}}_d$ by identifying $H^{\mathbb{R}}_d \cong \mathbb{R}^{N_d}$, where N_d is the number of coefficients of a generic homogeneous polynomial $f \in \mathbb{R}[X_0, \ldots, X_n]$ of degree d. We have

$$N_d = \binom{d+n}{n}.$$

We introduce a well-ordering in the set of multi-indices

$$\mathscr{M}on_d := \{(\mu_0, \ldots, \mu_n) : \mu_0 + \cdots + \mu_n = d\} \subseteq \mathbb{N}^{n+1}$$

as a bijection

$$\varphi : \mathscr{M}on_d \to \{1 \leqslant i \leqslant N_d\}.$$

The reader may assume that φ is given by the lexicographic order on $\mathscr{M}on_d$. Using this ordering we define the diagonal matrix Δ_d in the following terms:

$$\Delta_d \coloneqq \left(\binom{d}{\mu_0 \cdots \mu_n}^{-1/2} \right)_{1 \leqslant \varphi(\mu_0,\ldots,\mu_n) \leqslant N_d},$$

where

$$\binom{d}{\mu_0 \cdots \mu_n} \coloneqq \left(\frac{d!}{\mu_0! \cdots \mu_n!} \right).$$

For every list $(d) \coloneqq (d_1, \ldots, d_n) \in \mathbb{N}^n$ of degrees let $\mathscr{H}^{\mathbb{R}}_{(d)} \coloneqq H^{\mathbb{R}}_{d_1} \times \cdots \times H^{\mathbb{R}}_{d_n}$ be the space of sequences $F \coloneqq (f_1, \ldots, f_n)$ of homogeneous polynomials such that $f_i \in H^{\mathbb{R}}_{d_i}$, $1 \leqslant i \leqslant n$. We may also see $\mathscr{H}^{\mathbb{R}}_{(d)}$ as the space of all polynomial mappings $F \coloneqq (f_1, \ldots, f_n) : \mathbb{R}^{n+1} \to \mathbb{R}^n$, such that $f_i \in H^{\mathbb{R}}_{d_i}$, for all i. We denote by $\mathscr{H}^{\mathbb{Q}}_{(d)}$ the rational vector space given as the Cartesian product:

$$\mathscr{H}^{\mathbb{Q}}_{(d)} = H^{\mathbb{Q}}_{d_1} \times \cdots \times H^{\mathbb{Q}}_{d_n}.$$

We may extend the previous Euclidean inner product to the product space $\mathscr{H}^{\mathbb{R}}_{(d)}$ in the obvious terms: Given $F \coloneqq (f_1, \ldots, f_n) \in \mathscr{H}^{\mathbb{R}}_{(d)}$ and $G \coloneqq (g_1, \ldots, g_n) \in \mathscr{H}^{\mathbb{R}}_{(d)}$, we define the *canonical Hermitian inner product* on $\mathscr{H}^{\mathbb{R}}_{(d)}$ as $\langle \cdot, \cdot \rangle : \mathscr{H}^{\mathbb{R}}_{(d)} \times \mathscr{H}^{\mathbb{R}}_{(d)} \to \mathbb{R}$ in the following terms:

$$\langle F, G \rangle \coloneqq \sum_{i=1}^{n} \langle f_i, g_i \rangle.$$

For every $F \in \mathscr{H}^{\mathbb{R}}_{(d)}$, we denote by $||F||_2$ the norm defined by this canonical Hermitian inner product, i.e. $||F||_2 \coloneqq (\langle F, F \rangle)^{\frac{1}{2}}$.

On the other hand, let Δ be the matrix given as the diagonal sum of the matrices $\Delta_{d_1}, \ldots, \Delta_{d_n}$. Namely,

$$\Delta \coloneqq \Delta_{d_1} \oplus \cdots \oplus \Delta_{d_n}.$$

As in Section 3.1, we introduce the Euclidean inner product $\langle \cdot, \cdot \rangle_\Delta : \mathscr{H}^{\mathbb{R}}_{(d)} \times \mathscr{H}^{\mathbb{R}}_{(d)} \to \mathbb{R}$ defined by the non-singular matrix Δ. Namely, for every $F \in \mathscr{H}^{\mathbb{R}}_{(d)}$ and for every $G \in \mathscr{H}^{\mathbb{R}}_{(d)}$, we define $\langle F, G \rangle_\Delta$ as

$$\langle F, G \rangle_\Delta \coloneqq \langle \Delta F, \Delta G \rangle.$$

For every $F \in \mathscr{H}^{\mathbb{R}}_{(d)}$, we denote by $||F||_\Delta$ the norm defined by this canonical Hermitian inner product.

Let $O(n+1)$ be the orthogonal group of isometries of $\mathbb{R}^{n+1}$. We may define the action of the group $O(n+1)$ on $\mathscr{H}^{\mathbb{R}}_{(d)}$ in the following terms. Given $F \in \mathscr{H}^{\mathbb{R}}_{(d)}$ and given $\sigma \in O(n+1)$, we define $\sigma(F) \in \mathscr{H}^{\mathbb{R}}_{(d)}$ as the unique polynomial mapping in $\mathscr{H}^{\mathbb{R}}_{(d)}$

that satisfies the following identity:

$$\sigma(F)(x) \coloneqq F(\sigma^{-1}(x)), \quad \forall x \in \mathbb{R}^{n+1}.$$

Then, the following statements holds.

Theorem 19 (Blum et al. [5]). *This Hermitian inner product* $\langle \cdot, \cdot \rangle_{\Delta}$ *on* $\mathscr{H}^{\mathbb{R}}_{(d)}$ *is unitarily invariant. In other words,*

$$\langle \sigma(F), \sigma(G) \rangle_{\Delta} = \langle F, G \rangle_{\Delta},$$

for every $\sigma \in O(n+1)$ *and for every* $F, G \in \mathscr{H}^{\mathbb{R}}_{(d)}$.

As in Section 3.1 we have two Riemmanian structures in $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ accordingly to the corresponding Euclidean inner product in $\mathscr{H}^{\mathbb{R}}_{(d)}$. Let N be the (projective) dimension of $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$. Recall that the following equality holds:

$$N = \left(\sum_{i=1}^{n} \binom{n+d_i}{n} \right) - 1.$$

We may identify $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ with the real projective space $\mathbb{P}_N(\mathbb{R}) = \mathbb{P}(\mathbb{R}^{N+1})$. We denote by $(\mathbb{P}_N(\mathbb{R}), can)$ the Riemannian structure defined by the canonical Hermitian inner product $\langle \cdot, \cdot \rangle : \mathscr{H}^{\mathbb{R}}_{(d)} \times \mathscr{H}^{\mathbb{R}}_{(d)} \to \mathbb{R}$. We denote by $(\mathbb{P}_N(\mathbb{R}), \Delta)$ the Riemannian structure defined by the (unitarily invariant) Euclidean inner product $\langle \cdot, \cdot \rangle_{\Delta} : \mathscr{H}^{\mathbb{R}}_{(d)} \times \mathscr{H}^{\mathbb{R}}_{(d)} \to \mathbb{R}$ introduced above.

As in Section 3.1 we may associate two volume forms to $\mathbb{P}_N(\mathbb{R})$ accordingly to the corresponding Riemannian structure. For every subset $S \subseteq \mathbb{P}_N(\mathbb{R})$ we denote as $Vol_{\text{can}}(S)$ the volume of S with respect to the Riemannian structure $(\mathbb{P}_N(\mathbb{R}), can)$ and we denote as $Vol_{\Delta}(S)$ the corresponding volume of S with respect to the Riemannian structure $(\mathbb{P}_N(\mathbb{R}), \Delta)$.

4.2. Real and complex zeros

For every $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ we may define the complex projective algebraic variety $V_{\mathbb{C}}(F) \subseteq \mathbb{P}_n(\mathbb{C})$ by the following identity:

$$V_{\mathbb{C}}(F) \coloneqq \{z \in \mathbb{P}_n(\mathbb{C}) : f_i(z) = 0, \ 1 \leqslant i \leqslant n\}.$$

This is a non-empty variety. The real part $V_{\mathbb{R}}(F)$ of $V_{\mathbb{C}}(F)$ is defined as the set of real projective common zeros of $f_1, \ldots, f_n$. Namely

$$V_{\mathbb{R}}(F) \coloneqq \{z \in \mathbb{P}_n(\mathbb{R}) : f_i(z) = 0, \ 1 \leqslant i \leqslant n\}.$$

Let $S_{\infty} \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be the set of all systems of homogeneous equations $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ such that $\sharp(V_{\mathbb{R}}(F))$ is not a finite number. For every system $F \in S_{\infty}$ the complex projective variety $V_{\mathbb{C}}(F)$ is not a finite number of points. Hence, S_{∞} is included in a

projective algebraic subset of $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ and the following equality holds:

$$Vol_{can}(S_\infty) = Vol_\Delta(S_\infty) = 0.$$

For every integer number $k \in \mathbb{N}$ let $S_k \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be the set of all systems $F \in \mathbb{P}(\mathscr{H}_{(d)})$ such that

$$\sharp(V_{\mathbb{R}}(F)) = k < \infty.$$

For every list of degrees $(d) \coloneqq (d_1, \ldots, d_n)$ we denote by $D_{(d)}$ the positive integer number given by the following identity:

$$D_{(d)} \coloneqq \max\{n, d_1, \ldots, d_n\}.$$

Lemma 20. *Let $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be a system of polynomial equations and assume that $F \in S_k \backslash S_\infty$. Then, the following holds*:

- *Either $V_{\mathbb{C}}(F)$ is not a zero-dimensional projective variety, $k \leqslant D_{(d)}(2D_{(d)} - 1)^n$, and $Vol_\Delta(S_k) = 0$* or
- *$k \leqslant \mathscr{D}_{(d)} = \prod_{i=1}^n d_i$.*

In other words, for $k > \max\{D_{(d)}(2D_{(d)} - 1)^n, \mathscr{D}_{(d)}\}$, the set S_k is empty. From now on, we denote by

$$\mathscr{D}'_{(d)} \coloneqq \max\{D_{(d)}(2D_{(d)} - 1)^n, \mathscr{D}_{(d)}\}.$$

The following Theorem was shown in [48] (cf. also [5]).

Theorem 21 (Shub and Smale [48]). *With the same notations as above, the following equality holds*:

$$\sum_{k=0}^{\infty} \frac{k Vol_\Delta(S_k)}{Vol_\Delta(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))} = \sum_{k=0}^{\mathscr{D}_{(d)}} \frac{k Vol_\Delta(S_k)}{Vol_\Delta(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))} = (\mathscr{D}_{(d)})^{1/2},$$

where $\mathscr{D}_{(d)} \coloneqq \prod_{i=1}^n d_i$ is the Bézout number.

4.3. Some elimination theory

With the same notations as in previous subsections, for every $k \in \mathbb{N} \cup \{\infty\}$, the cone $\widetilde{S_k} \subseteq \mathscr{H}^{\mathbb{R}}_{(d)}$ over S_k is a semi-algebraic set. We are interested on quantifier free formulae that describe the semi-algebraic set $\widetilde{S_k}$.

In the rest of the section we identify $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ and $\mathbb{P}_N(\mathbb{R})$. This can be done by identifying every list $F \coloneqq (f_1, \ldots, f_n) \in \mathscr{H}^{\mathbb{R}}_{(d)}$ and the list of its coefficients $(z_0, \ldots, z_N) \in \mathbb{R}^{N+1}$. In particular, for every homogeneous polynomial

$q \in \mathbb{R}[Z_0, \ldots, Z_n]$ and for every $F := (f_1, \ldots, f_n) \in \mathscr{H}^{\mathbb{R}}_{(d)}$, we denote by $q(F) \in \mathbb{R}$ the real number obtained by evaluating the polynomial q at the list of coefficients of F.

We prove the following statement:

Theorem 22. *There are universal constants $A, C > 0$ such that the following holds*:

For every list of degrees $(d) := (d_1, \ldots, d_n)$ there is a finite set of polynomials $\mathscr{F}_{(d)} := \{K_0, \ldots, K_s\} \subseteq \mathbb{Q}[Z_0, \ldots, Z_N]$ such that the following holds:

(1) $s \leqslant AD^{Cn}_{(d)}$,

(2) $\deg(K_i) \leqslant 2D^{Cn}_{(d)}$.

(3) *There is complex projective algebraic variety $W_\infty \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ such that $W_\infty \supseteq S_\infty$* and

$$Vol_\Delta(W_\infty) = Vol_\Delta(S_\infty) = 0.$$

The projective algebraic variety W_∞ is given by the following identity:

$$W_\infty := \{F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}) : K_0(F) = 0\}.$$

(4) *For every k, $0 \leqslant k \leqslant \mathscr{D}'_{(d)}$, there is a subset $W_k \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ such that the following holds*:

(a) *The cone $\widetilde{W_k}$ over W_k is a $\mathscr{F}_{(d)}$-definable semi-algebraic subset of $\mathbb{R}^{N+1}$*,

(b) *$W_k \subseteq S_k$ and the following inclusion holds*:

$$S_k \setminus W_k \subseteq W_\infty,$$

(c) $Vol_\Delta(W_k) = Vol_\Delta(S_k)$.

The constants A and C of Theorem 22 above come from the elimination theory method used to prove the Theorem (i.e. from the algorithm described in [32]). They are large. For instance, $C < 87$ and $\log_{10} A < 7.36$ is the estimate coming from [32]. They could be improved using either a refinement of the algorithm in [32] or using alternative elimination procedures as those in the series of papers [19–22,25]. Either technical refinements in elimination theory (as those in [23,34,29]) or using specific elimination methods for real closed fields (as those in [1,2] or those of [3]). However, small improvements on the exponents A and C do not change significantly the estimates of this Theorem 22 and we choose the simplest and more direct technique.

The proof of the theorem is based on three main topics:

(1) The existence of correct-test-sequences as those introduced in [30] and their improvements in [32].

(2) The existence of efficient elimination procedures as those discussed above.

(3) The use of sub-resultant techniques (as introduced by Habicht in [24] and re-discovered by Collins in [14]). Meaningful refinements (as those by Lickteig and Roy in [35]) can also help to improve the constants A and C in Theorem 22

above. As in the case of elimination methods, these potential improvements do not significantly change the statement or the proof.

In order to keep the proof of this theorem within the short margin of a paper, we just recall some basic facts concerning these three topics and then we give a sketch of the proof of the theorem in Section 4.5 below.

4.3.1. Some elimination theory

This subsection is devoted to recall some basic statements concerning degrees and complexities of some elimination polynomials. The basis is the existence of consistency tests for systems of homogeneous polynomial equations. These consistency tests, as the Cayley–Chow form, are multivariate polynomials in the coefficients of the given system of equations. Bounds in the degrees and the evaluation complexity of the elimination polynomials of these consistency tests were achieved in Section 4.8 of [32] (see also [18, Section 3]). We omit most of the proofs which are simply a rewriting of some of the technical statements contained in Refs. [32,18]. The reader may easily reconstruct the polynomials considered.

Lemma 23 (Krick and Pardo [32, Section 4.8]). *There is a universal constant* $c>0$, $(c<20)$ *such that the following holds*:

For every list $(d)=(d_1,\ldots,d_n)$ *of degrees and for every positive integer number* r, $1\leqslant r\leqslant n$, *there is a non-zero polynomial* $K_r\in\mathbb{Z}[Z_0,\ldots,Z_N]$ *such that the following holds*:

(1) $\deg(K_r)\leqslant D_{(d)}^{cn}$,
(2) *for every* $F\in\mathscr{H}_{(d)}^{\mathbb{R}}$, *the complex projective variety* $V_{\mathbb{C}}(F)$ *has dimension greater than* r, *then* $K_r(F)=0$.
(3) *There is a non-scalar straight-line program* Γ *of size* $D_{(d)}^{cn}$ *and non-scalar depth* $cn\log_2 D_{(d)}$ *that evaluates* K_r.

Let $K\in\mathbb{Q}[Z_0,\ldots,Z_N]$ be the polynomial of degree at most $nD_{(d)}^{cn}$ given by the following identity:

$$K:=\prod_{i=1}^{n}K_r\in\mathbb{Q}[Z_0,\ldots,Z_N]. \tag{28}$$

This polynomial satisfies the following property: *For every* $F\in\mathscr{H}_{(d)}^{\mathbb{R}}$, *if* $K(F)\neq 0$, *then* $V_{\mathbb{C}}(F)$ *is a finite set* (*i.e. a zero-dimensional projective variety*). Observe that the polynomial K can be evaluated by a non-scalar straight-line program of size $nD_{(d)}^{cn}$ and non-scalar depth $cn(\log_2 D_{(d)}+1)$.

Using again the estimates of [32,18] we can estimate both degrees and complexity of the polynomials occurring in the next statement. Again, we omit the proof, which adds nothing significant to our text here, and the reader may follow the details in both references.

Lemma 24. *With the same notations as in Lemma 23 above, there is a polynomial* $R \in \mathbb{Z}[Z_0, \ldots, Z_N, T_0, \ldots, T_n]$ *of degree at most* $D_{(d)}^{cn}$ *such that the following holds*:

For every $F \in \mathscr{H}_{(d)}^{\mathbb{R}}$ *and for every* $\underline{\lambda} := (\lambda_0, \ldots, \lambda_n) \in \mathbb{R}^{n+1}$, *if* $K(F) \neq 0$ *and* $R(F, \underline{\lambda}) \neq 0$, *then no projective point in* $V_{\mathbb{C}}(F)$ *belongs to the linear projective hyperplane*:

$$H_{\underline{\lambda}} := \{(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}_n(\mathbb{C}) : \lambda_0 x_0 + \cdots + \lambda_n x_n = 0\}.$$

The polynomial R *can be evaluated by a non-scalar straight-line program* Γ_1 *of size* $D_{(d)}^{cn}$ *and non-scalar depth* $cn \log_2 D_{(d)}$.

For every $\underline{\lambda}, \underline{\mu} \in \mathbb{R}^{n+1}$, we denote by $U_{\underline{\lambda},\underline{\mu}}$ the mapping

$$U_{\underline{\lambda},\underline{\mu}} : \mathbb{P}_n(\mathbb{C}) \backslash H_{\underline{\lambda}} \to \mathbb{C},$$

such that for every $(x_0 : \cdots : x_n) \in \mathbb{P}_n(\mathbb{C}) \backslash H_{\underline{\lambda}}$, the complex number $U_{\underline{\lambda},\underline{\mu}}(x_0 : \ldots : x_n) \in \mathbb{C}$ is given by the following identity:

$$U_{\underline{\lambda},\underline{\mu}}(x_0 : \ldots : x_n) := \frac{\mu_0 x_0 + \cdots + \mu_n x_n}{\lambda_0 x_0 + \cdots + \lambda_n x_n} \in \mathbb{C}.$$

Finally, we introduce the last family of elimination polynomials that we use in these pages. The exhibited bounds on degrees and complexity easily follows from the techniques of [32,18].

Lemma 25. *With the same notations as in previous statements, there are polynomials*

$$L, A_0, \ldots, A_{\mathscr{D}_{(d)}} \in \mathbb{Z}[Z_0, \ldots, Z_N, T_0, \ldots, T_n, Y_0, \ldots, Y_n],$$

such that the following holds:

(1) $\deg(L) \leqslant D_{(d)}^{cn}$.

(2) *For every* i, $0 \leqslant i \leqslant \mathscr{D}_{(d)}$, $\deg(A_i) \leqslant D_{(d)}^{cn}$.

(3) *There is a non-scalar straight-line program* Γ_2 *of size* $D_{(d)}^{cn}$ *and depth* $cn \log_2 D_{(d)}$ *that evaluates the polynomial* L *and the polynomials* $A_0, \ldots A_{\mathscr{D}_{(d)}}$.

(4) *For every* $F \in \mathscr{H}_{(d)}^{\mathbb{R}}$ *and for every* $\underline{\lambda}, \underline{\mu} \in \mathbb{R}^{n+1}$, *if* $K(F) \neq 0$, $R(F, \underline{\lambda}) \neq 0$, *and* $L(F, \underline{\lambda}, \underline{\mu}) \neq 0$, *the mapping* $U_{\underline{\lambda},\underline{\mu}}$ *defines a bijection between* $V_{\mathbb{C}}(F)$ *and the complex roots of the univariate polynomial*:

$$P(F, \underline{\lambda}, \underline{\mu}, X) := \sum_{i=1}^{\mathscr{D}_{(d)}} A_i(F, \underline{\lambda}, \underline{\mu}) X^i.$$

(5) *Moreover, for every* $F \in \mathscr{H}_{(d)}^{\mathbb{R}}$ *and for every* $\underline{\lambda}, \underline{\mu} \in \mathbb{R}^{n+1}$, *if* $K(F) \neq 0$, $R(F, \underline{\lambda}) \neq 0$, *and* $L(F, \underline{\lambda}, \underline{\mu}) \neq 0$, *the mapping* $U_{\underline{\lambda},\underline{\mu}}$ *defines a bijection between the real solutions in* $V_{\mathbb{R}}(F)$ *and the real solutions* $x \in \mathbb{R}$ *of the polynomial equation* $P(F, \underline{\lambda}, \underline{\mu}, x) = 0$.

4.3.2. Adding correct-test sequences to elimination polynomials

In order to achieve the proof of Theorem 22 we combine the existence of elimination polynomials introduced in the previous subsection with the existence of correct-test sequences as introduced in [30] and improved in [32].

Definition 26. Given a set $\mathscr{F} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ (which contains the null polynomial) we say that a finite set $\mathscr{Q} \subseteq \mathbb{Z}^n$ is a questor (or a correct test sequence) *for* $\mathscr{F}$ iff for all $P \in \mathscr{F}$ the following holds:

$$P|_{\mathscr{Q}} = 0 \Rightarrow P \equiv 0.$$

The following lemma gives estimates on correct-test sequences in terms of degrees and complexity.

Lemma 27 (Krick and Pardo [32]). *Let $n, \ell, L \in \mathbb{N}$, $L \geqslant n+1$ be positive integer numbers. Let Γ_0 be a non-scalar straight-line program of size L, depth ℓ that evaluates polynomials in $\mathbb{Z}[X_0, \ldots, X_n]$. Let $u, Q \in \mathbb{Z}$ be the positive integer numbers given by the following identity*:

$$u := (2^{\ell+1} - 2)(2^{\ell} + 1)^2 \quad \text{and} \quad Q := 6\,(\ell L)^2.$$

Let $\mathscr{F} \subseteq \mathbb{Z}[X_0, \ldots, X_n]$ be a finite set of polynomials evaluable by Γ_0. Then the set $\{1, \ldots, u\}^{n+1} \subseteq \mathbb{Z}^{n+1}$ contains at least $u^{nt}(1 - u^{-\frac{Q}{6}})$ correct test sequences of length Q for $\mathscr{F}$.

Therefore it contains at least one correct test sequence of this length. Combining this last statement with Lemmas 23, 24 and 25 we get

Proposition 28. *Let $(d) := (d_1, \ldots, d_n)$ be a list of degrees and let notations and assumptions be as in Lemmas* 23, 24 *and* 25 *above. In particular, let $c > 0$ be the constant introduced in Lemma* 23. *Let $u, Q \in \mathbb{N}$ be the positive integer numbers given by the following identity*:

$$u := 2(2D_{(d)}^{cn} + 1)^3, \quad Q := 6(cn \log_2 D_{(d)} + 1)^2 D_{(d)}^{2cn}.$$

Then, there is a finite subset $\mathscr{Q} \subseteq \{1, \ldots, u\}^{n+1}$ such that $\sharp(\mathscr{Q}) = Q$ and such that the following property holds:

For every $F \in \mathscr{H}_{(d)}^{\mathbb{R}}$ such that $K(F) \neq 0$, there is $(\underline{\lambda}, \underline{\mu}) \in \mathscr{Q}^2$ such that

$$R(F, \underline{\lambda})L(F, \underline{\lambda}, \underline{\mu}) \neq 0.$$

4.3.3. Subresultants and sturm theorem

Subresultant theory was implicitly used in [24] and explicitely introduced by Collins in [14] and Loos in [37]; see also [7–9]. We just need some basic facts from subresultants and their application to the computation of the Cauchy index of a rational function. The reader may follow more detailed studies in [45] and the excellent algorithm described in [35].

Let $f \coloneqq \sum_{i=0}^{D} a_i X^i \in \mathbb{R}[X]$ be a univariate polynomial of degree D and let $f' \in \mathbb{R}[X]$ its derivative. Let $S \coloneqq Sylv(f,f') \in \mathscr{M}_{2D-1}(\mathbb{R})$ be the Sylvester matrix of f and f'. Let us introduce the remainder sequence of Euclid's algorithm when applied to f and f':

$$\begin{aligned}
f &= q_0 f' + r_0 \\
g &= q_1 r_0 + r_1 \\
r_0 &= q_2 r_1 + r_2 \\
&\vdots \\
r_{i-2} &= q_i r_{i-1} + r_i \\
&\vdots \\
r_{\ell-2} &= q_\ell r_{\ell-1} + r_\ell \\
r_{\ell-1} &= q_{\ell+1} r_\ell .
\end{aligned}$$

For every i, $0 \leqslant i \leqslant \ell$, let $n_j \coloneqq \deg(r_j)$ be the degree of the ith remainder r_i. We define the *degree sequence associated to f and f'* as the following sequence of positive integer numbers:

$$D > D-1 > n_0 > n_1 > n_2 > \cdots > n_\ell .$$

The following theorem explains the relevance of subresultant theory:

Theorem 29. *Let $k \in \mathbb{N}$ be a non-negative integer number, $0 \leqslant k \leqslant D-1$. There is a polynomial $\sigma_k^D \in \mathbb{Q}[A_0, \ldots, A_D]$ of degree at most $2D-1$ such that for every polynomial $f \coloneqq \sum_{k=0}^{D} a_i X^i \in \mathbb{R}[X]$ of degree D the following inequality holds*:

$$\sigma_k^D(a_0, \ldots, a_D) \neq 0 \iff k \text{ appears in the degree sequence of } f \text{ and } f'.$$

The polynomial σ_k^D is called the kth subresultant of a generic polynomial of degree D.

The kth subresultant σ_k^D is given as the determinant of a submatrix S_k^D of the Sylvester matrix $Sylv(f,f')$. In fact, the submatrix S_k^D is given by a combinatorial rule that only depends on D and k.

Let $\mathscr{R}_D \coloneqq \{\sigma_k^D \in \mathbb{Q}[A_0, \ldots, A_D] : 0 \leqslant k \leqslant D-1\}$ be the finite set of all subresultant polynomials of a generic polynomial of degree D.

Let $\mathbb{R}[X]_D \coloneqq \mathbb{R}^{D+1}$ be the real vector space of all univariate polynomials with real coefficients of degree at most D, and let $\mathscr{P}_D \subseteq \mathbb{R}[X]_D$ be the semi-algebraic subset of all polynomials of degree D.

Let $\underline{\epsilon} \coloneqq (\epsilon_0, \ldots, \epsilon_D) \in \{>, =, <\}^{D+1}$ be a sign sequence. Let $\mathscr{P}_{D,\underline{\epsilon}}$ be the $\mathscr{R}_D$-definable semi-algebraic cell in $\mathbb{R}^{D+1}$ given by the following identity:

$$\mathscr{P}_{D,\underline{\epsilon}} \coloneqq \left\{ f \coloneqq \sum_{i=0}^{D} a_i X^i : \sigma_k^D(a_0, \ldots, a_D) \epsilon_k 0,\ 0 \leqslant k \leqslant D-1 \right\}.$$

The following statement also holds:

Theorem 30. *Let $D \in \mathbb{N}$ be a degree bound and let $\underline{\epsilon} \in \{>, =, <\}^{D+1}$ be a sign sequence determining the semi-algebraic set $\mathscr{P}_{D,\underline{\epsilon}} \subseteq \mathbb{R}^{D+1}$. Then, there is only one degree sequence*

$$D > D-1 > n_0 > n_1 > n_2 > \cdots > n_l,$$

depending only on D and $\underline{\epsilon}$, such that it is the degree sequence associated to any polynomial $f \in \mathscr{P}_{D,\underline{\epsilon}}$.

In order to apply Sturm's theorem (as described in [45], for instance) we just need to determine the signs of the leading coefficients of the remainder sequence of f and f'. The following statements relates subresultants and remainders.

Lemma 31. *Let $D \in \mathbb{N}$ be a positive integer number and $k \in \mathbb{N}$ a positive integer number such that $0 \leqslant k \leqslant D-1$. Then, there are polynomials $\rho^0_{k,D}, \ldots, \rho^k_{k,D} \in \mathbb{Q}[A_0, \ldots, A_D]$ of degree at most $2D$ such that the following holds*:

For every polynomial $f := \sum_{i=0}^{D} a_i X^i \in \mathbb{R}[X]$ of degree D such that

$$\sigma^D_k(a_0, \ldots, a_D) \neq 0,$$

there is a polynomial $r_i \in \mathbb{R}[X]$ in the remainder sequence of f and f' such that $\deg(r_i) = k$, and the following equality holds:

$$r_i := \sigma^D_k(a_0, \ldots, a_D)^{-1}(\rho^0_{k,D}(a_0, \ldots, a_D) + \cdots + \rho^k_{k,D}(a_0, \ldots, a_D)X^k).$$

Finally, let us define the finite set of polynomials:

$$\tilde{\mathscr{R}}_D := \mathscr{R}_D \cup \left(\bigcup_{k=0}^{D-1} \{\rho^0_{k,D}, \ldots, \rho^k_{k,D}\} \right) \subseteq \mathbb{Q}[A_0, \ldots, A_D].$$

This family of multivariate polynomials yields the following statement:

Theorem 32. *Let $D \in \mathbb{N}$ be a positive integer number, let $r \in \mathbb{N}$ be a positive integer number such that $0 \leqslant r \leqslant D$, and let $\tilde{\mathscr{R}}_D$ be the finite set of polynomials defined above. Then, the semi-algebraic set of all polynomials $f \in \mathbb{R}[X]$ of degree D with exactly r different real roots is $\tilde{\mathscr{R}}_D$-definable. In fact, for every $\tilde{\mathscr{R}}_D$-cell in $\mathscr{P}_D$ the number of real roots of any polynomial $f \in \mathscr{P}_D$ is constant.*

4.3.4. Proof of Theorem 22

Let $(d) := (d_1, \ldots, d_n)$ be a list of degrees and let k be a non-negative integer number $0 \leqslant k \leqslant \mathscr{D}_{(d)}$. Let $W_k \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be the set of all systems of homogeneous polynomial equations $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ such that $K(F) \neq 0$ and $\sharp(V_{\mathbb{R}}(F)) = k$, where $K \in \mathbb{Q}[Z_0, \ldots, Z_N]$ is the polynomial introduced in Identity (28) above. We define

$$W_\infty := \{F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}) : K(F) = 0\}.$$

Let $\mathscr{Q} \subseteq \mathbb{Z}^{n+1}$ be the correct-test sequence defined in Proposition 28. In order to simplify notations, we shall write $\underline{Z}$ to denote the list of variables $(Z_0, \ldots, Z_N)$. Let $\mathscr{F} \subseteq \mathbb{Z}[\underline{Z}]$ be the finite set of polynomials given by the following equality:

$$\mathscr{F} := \{K_0\} \cup \mathscr{F}_1 \cup \mathscr{F}_2 \cup \mathscr{F}_3 \cup \mathscr{F}_4, \tag{29}$$

where

- $K_0 = K$, where K is the polynomial introduced in Identity (28),
- $\mathscr{F}_1 \subseteq \mathbb{Z}[\underline{Z}]$ is the finite set of polynomials given by the following equality:

  $$\mathscr{F}_1 := \{R(\underline{Z}, \underline{\lambda}) L(\underline{Z}, \underline{\lambda}, \underline{\mu}) : (\underline{\lambda}, \underline{\mu}) \in \mathscr{Q}^2\},$$

  where $R(\underline{Z}, \underline{\lambda})$ is the polynomial defined in Lemma 24 and $L(\underline{Z}, \underline{\lambda}, \underline{\mu})$ is the polynomial defined in Lemma 25.
- $\mathscr{F}_2 \subseteq \mathbb{Z}[\underline{Z}]$ is the finite set of polynomials given by the following equality:

  $$\mathscr{F}_2 := \{A_k(\underline{Z}, \underline{\lambda}, \underline{\mu}) : 0 \leqslant k \leqslant \mathscr{D}_{(d)}, (\underline{\lambda}, \underline{\mu}) \in \mathscr{Q}^2\},$$

  where the polynomials $A_k(\underline{Z}, \underline{\lambda}, \underline{\mu})$ are the polynomials introduced in Lemma 25 and $\mathscr{D}_{(d)} := \prod_{i=1}^{n} d_i$ is the Bézout number of the list of degrees (d).
- $\mathscr{F}_3 \subseteq \mathbb{Z}[\underline{Z}]$ is the finite set of polynomials given by the following equality:

  $$\mathscr{F}_3 := \{\sigma_k^D(A_0(\underline{Z}, \underline{\lambda}, \underline{\mu}), \ldots, A_D(\underline{Z}, \underline{\lambda}, \underline{\mu})):$$
  $$0 \leqslant k \leqslant D-1, 0 \leqslant D \leqslant \mathscr{D}_{(d)}, (\underline{\lambda}, \underline{\mu}) \in \mathscr{Q}^2\},$$

  where σ_k^D is the kth subresultant for polynomials of degree D introduced in Theorem 29 above.
- $\mathscr{F}_4 \subseteq \mathbb{Z}[\underline{Z}]$ is the finite set of polynomials given by the following equality:

  $$\mathscr{F}_4 := \{\rho_{k,D}^j(A_0(\underline{Z}, \underline{\lambda}, \underline{\mu}), \ldots, A_D(\underline{Z}, \underline{\lambda}, \underline{\mu})):$$
  $$0 \leqslant j \leqslant k, 0 \leqslant k \leqslant D-1, 0 \leqslant D \leqslant \mathscr{D}_{(d)}, (\underline{\lambda}, \underline{\mu}) \in \mathscr{Q}^2\},$$

  where $\rho_{k,D}^j$ are the polynomials introduced in Lemma 31 above.

The statements described in Sections 4.3.1 and 4.3.3 above, imply that for every k, $0 \leqslant k \leqslant \mathscr{D}_{(d)}$ the cone $\widetilde{W_k}$ over W_k is $\mathscr{F}$-definable. The cone $\widetilde{W_\infty}$ over W_∞ is given as

$$\widetilde{W_\infty} = \{F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{R}}) : K_0(F) = 0\}.$$

From the upper degree bounds stated in Sections 4.3.1 and 4.3.3 we easily conclude that for every polynomial $K_i \in \mathscr{F}$ the following inequality holds:

$$\deg(K_i) \leqslant 2D_{(d)}^{cn} \mathscr{D}_{(d)}.$$

Finally, Equality (29) implies that the number s of polynomials in $\mathscr{F}$ satisfies the following inequality:

$$s \leqslant 6^2 (cn \log_2 D_{(d)} + 1)^4 D_{(d)}^{4cn} (3\mathscr{D}_{(d)} + 1)^3 + 1) + 1.$$

Finally, taking $A \coloneqq 6^2 4c^4$ and $C \coloneqq 4c+7$, the following inequality also holds:

$$s \leqslant AD_{(d)}^{Cn}.$$

This achieves the sketch of the proof of Theorem 22. □

4.4. Unitarily invariant bit length of systems of polynomial equations

In Section 3, Definition 17, we introduced the notion of Northcott–Schmidt logarithmic height of a projective point $x \in \mathbb{P}_m(\mathbb{Q})$. We also discussed that the logarithmic height of a projective point may be interpreted as the bit length required to represent $x \in \mathbb{P}_m(\mathbb{Q})$ in a Turing machine. For systems of homogeneous multivariate polynomial equations $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$, we slightly modify this notion of bit length because of technical reasons. The reader should observe that this new notion of "bit length" (that we call "unitarily invariant bit length of a system $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$") is, up to a constant factor, equivalent to Northcott–Schmidt's logarithmic height.

As in Section 3.3, let $\mathscr{P} \subseteq \mathbb{N}$ be the set of all prime positive integer numbers. For every $p \in \mathscr{P}$, let $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ be the non-Archimedean absolute value.

Definition 33. For every $F \coloneqq [z_0 : \cdots : z_N] \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$, we define the unitarily invariant (absolute) height of F as

$$H_{\Delta}(F) \coloneqq ||F||_{\Delta} \prod_{p \in \mathscr{P}} \max\{|z_i|_p : 0 \leqslant i \leqslant N\},$$

where Δ is the diagonal matrix introduced in Section 4.1. We define the unitarily invariant bit length of $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ as the logarithm of the unitarily invariant absolute height. Namely,

$$bl_{\Delta}(F) \coloneqq \log H_{\Delta}(F).$$

As discussed in the preamble of this Section the unitarily invariant bit length of a system of homogeneous polynomial equations $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ is equivalent (up to a constant factor) to Northcott–Schmidt's logarithmic height $ht(F)$. Namely, we have

$$ht(F) - \frac{D_{(d)} \log D_{(d)}}{2} \leqslant bl_{\Delta}(F) \leqslant ht(F),$$

where $D_{(d)} \coloneqq \max\{d_1, \ldots, d_n\}$. For instance, for quadratic systems (i.e. $(d) \coloneqq (2, 2, \ldots, 2)$) both quantities agree. This inequality easily follows from Definitions 17, 33 and the Definition of the diagonal matrix Δ in Section 4.1.

For every subset $S \subseteq \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{R}})$ and for every non-negative real number $h \geqslant 0$, we are interested on precise estimates for the number of rational points in S of unitarily invariant bit length at most h. Namely, we are interested on estimates for the quantity:

$$\mathscr{N}_{\Delta}(S, h) \coloneqq \sharp(\{F \in S : bl_{\Delta}(F) \leqslant h\}).$$

Observe that the following identity holds:

$$\mathscr{N}_{\Delta}(S,h)=\mathscr{N}_{\Delta}(S,\mathbb{Z}^{N+1},2^h),$$

where $\mathscr{N}_{\Delta}(S,\mathbb{Z}^{N+1},2^h)$ is the quantity introduced in Theorem 14. In fact, we are interested on estimates for $\mathscr{N}_{\Delta}(S_k,h)$ where $S_k\subseteq\mathbb{P}(\mathscr{H}_{(d)})$, $0\leqslant k\leqslant+\infty$ are the sets introduced in Section 4.2 above.

Theorem 34. *Let $A,C>0$ be the universal constants of Theorem 22 above. Then, the following holds*:

Let $(d):=(d_1,\ldots,d_n)$ be a list of degrees, $D_{(d)}:=\max\{n,d_1,\ldots,d_n\}$, $\mathscr{D}_{(d)}:=\prod_{i=1}^{n}d_i$, and let $\mathscr{D}'_{(d)}$ be the maximum:

$$\mathscr{D}'_{(d)}:=\max\{D_{(d)}(2D_{(d)}-1)^n,\mathscr{D}_{(d)}\}.$$

Then, the following inequalities hold for every non-negative real number $h\in\mathbb{R}$:

(1) *For every k, $0\leqslant k\leqslant\mathscr{D}_{(d)}$, the following inequality holds*:

$$|\mathscr{N}_{\Delta}(S_k,h)-\mathscr{V}_{(d)}(k)2^{h(N+1)}|\leqslant\mathfrak{R}_{(d)}2^{hN},$$

where

$$\mathscr{V}_{(d)}(k):=\frac{Vol_{\Delta}(S_k)}{(N+1)|\det(\Delta)|\zeta(N+1)},$$

and

$$\mathfrak{R}_{(d)}:=(D_{(d)}!)^{\frac{N+1}{2}}[T(AD_{(d)}^{Cn},2D_{(d)}^{Cn},N+1)+K_{N+1}+1].$$

(2) *For every k, $\mathscr{D}_{(d)}<k\leqslant\mathscr{D}'_{(d)}$, the following inequality holds*:

$$|\mathscr{N}_{\Delta}(S_k,h)|\leqslant\mathfrak{R}_{(d)}2^{hN}.$$

(3) *For every k, $\mathscr{D}'_{(d)}<k<\infty$, the following equality holds*:

$$\mathscr{N}_{\Delta}(S_k,h)=0.$$

(4) *For $k=\infty$, the following inequality also holds*:

$$|\mathscr{N}_{\Delta}(S_\infty,h)|\leqslant\mathfrak{R}_{(d)}2^{hN}.$$

(5) *Finally, the following inequality also holds*:

$$|\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)-\mathscr{V}_{(d)}2^{h(N+1)}|\leqslant\mathscr{R}_{(d)}2^{hN},$$

where

$$\mathscr{V}_{(d)}:=\frac{Vol_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))}{(N+1)|\det(\Delta)|\zeta(N+1)},$$

and

$$\mathscr{R}_{(d)} \coloneqq (D_{(d)}!)^{\frac{N+1}{2}}[\mathfrak{S}^{(N+1)} + K_{N+1} + 1].$$

Proof. Let A, C be the positive constants introduced in Theorem 22 above. Let $\mathscr{F}_{(d)} = \{K_0, \ldots, K_s\} \subseteq \mathbb{Q}[Z_0, \ldots, Z_N]$ be the finite set of polynomials introduced in this Theorem 22. Then, there is a finite sequence

$$W_0, \ldots, W_{\mathscr{D}_{(d)}}, W_\infty,$$

of subsets of $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ such that the following properties hold:

(1) For every k, $0 \leqslant k \leqslant D_{(d)}$ or $k = \infty$, $\tilde{W}_k$ is $\mathscr{F}_{(d)}$-definable.
(2) $W_\infty \subseteq S_\infty$, and $Vol_\Delta(W_\infty) = Vol_\Delta(S_\infty) = 0$.
(3) For every k, $0 \leqslant k \leqslant \mathscr{D}_{(d)}$, $W_k \subseteq S_k$ and $S_k \backslash W_k \subseteq W_\infty$.
(4) For every k, $\mathscr{D}_{(d)} < k \leqslant \mathscr{D}'_{(d)}$, $S_k \subseteq W_\infty$ and $Vol_\Delta(S_k) = 0$.

From these properties we conclude the following inequalities:

- For every k, $0 \leqslant k \leqslant \mathscr{D}_{(d)}$, the following holds:

$$|\mathscr{N}_\Delta(S_k, h) - \mathscr{N}_\Delta(W_k, k)| \leqslant \mathscr{N}_\Delta(W_\infty, h).$$

- For every k, $\mathscr{D}_{(d)} < k \leqslant \mathscr{D}'_{(d)}$, the following inequality holds:

$$|\mathscr{N}_\Delta(S_k, h)| \leqslant \mathscr{N}_\Delta(W_\infty, h).$$

From Theorem 14, Theorem 22 and the Definition of Δ in Section 4.1 we easily conclude the following estimates:

For every k, $0 \leqslant k \leqslant \mathscr{D}_{(d)}$, the following holds:

$$|\mathscr{N}_\Delta(W_k, h) - \mathscr{V}_{(d)}(k) 2^{h(N+1)}| \leqslant \mathfrak{R}_{(d)} 2^{hN},$$

where

$$\mathscr{V}_{(d)}(k) \coloneqq \frac{Vol_\Delta(S_k)}{(N+1)|\det(\Delta)|\zeta(N+1)} = \frac{Vol_\Delta(W_k)}{(N+1)|\det(\Delta)|\zeta(N+1)}$$

and

$$\mathfrak{R}_{(d)} \coloneqq (D_{(d)}!)^{\frac{N+1}{2}}[T(AD^{Cn}_{(d)}, 2D^{Cn}_{(d)}, N+1) + K_{N+1} + 1].$$

As $Vol_\Delta(W_\infty) = 0$, the same statements yield the following inequality:

$$|\mathscr{N}_\Delta(W_\infty, h)| \leqslant \mathfrak{R}_{(d)} 2^{hN}.$$

The inequalities in the statement of the theorem follow from the claims used in this proof. □

4.5. Proof of Theorem 4

First of all, we prove the following technical lemma which is going to be used in the proof of Theorem 4.

Lemma 35. *With the same notations as above, let* $\mathfrak{W}_{(d)}$ *be the constant given by the following identity*:

$$\mathfrak{W}_{(d)} \coloneqq \frac{\mathscr{V}_{(d)}}{\mathfrak{R}_{(d)}}. \tag{30}$$

Let $h \in \mathbb{R}$ *be such that* $2^{h-1} \geqslant \mathfrak{W}_{(d)}^{-1}$. *Then, the following inequalities hold*:

(1) *for every* (d), *the following holds*:

$$\frac{\mathscr{N}_{\Delta}(S_\infty, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}), h)} \leqslant \frac{1}{\mathfrak{W}_{(d)} 2^h - 1}.$$

(2) *for every* (d), *the following holds*:

$$\left| \sum_{k \in \mathbb{N}} \frac{k \mathscr{N}_{\Delta}(S_k, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}), h)} - \sqrt{\mathscr{D}_{(d)}} \right| \leqslant \frac{(\mathscr{D}'_{(d)} + 1)^2 + \sqrt{\mathscr{D}_{(d)}}}{\mathfrak{W}_{(d)} 2^{h-1} - 1}.$$

Proof. The first claim follows from the following elementary argument:

$$\frac{\mathscr{N}_{\Delta}(S_\infty, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}), h)} \leqslant \frac{\mathfrak{R}_{(d)} 2^{hN}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}), h)}.$$

From Theorem 34 the following inequality holds:

$$\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}), h) \geqslant \mathscr{V}_{(d)} 2^{h(N+1)} - \mathscr{R}_{(d)} 2^{hN}. \tag{31}$$

As $\mathfrak{R}_{(d)} \geqslant \mathscr{R}_{(d)}$, we conclude

$$\frac{\mathscr{N}_{\Delta}(S_\infty, h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}), h)} \leqslant \frac{\mathfrak{R}_{(d)} 2^{hN}}{\mathscr{V}_{(d)} 2^{h(N+1)} - \mathfrak{R}_{(d)} 2^{hN}} \leqslant \frac{1}{\mathfrak{W}_{(d)} 2^h - 1}.$$

As for the second Claim, observe that the following equality holds for every $k \in \mathbb{N}$:

$$\frac{\mathscr{V}_{(d)}(k)}{\mathscr{V}_{(d)}} = \frac{Vol_{\Delta}(S_k)}{Vol_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))}.$$

Thus, from Theorem 21, the following also holds:

$$\Sigma_1 \coloneqq \left| \sum_{k \in \mathbb{N}} \frac{k \mathscr{V}_{(d)}(k) 2^{h(N+1)}}{\mathscr{V}_{(d)} 2^{h(N+1)}} - \sqrt{\mathscr{D}_{(d)}} \right| = 0.$$

Next, for every $k\in\mathbb{N}$, the following inequality also holds:

$$\left|\frac{\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))}-\frac{\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{V}_{(d)}2^{h(N+1)}}\right|\leqslant\frac{\mathscr{V}_{(d)}(k)\mathscr{R}_{(d)}2^{hN}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)\mathscr{V}_{(d)}}.$$

From Eq. (31) we conclude

$$\left|\frac{\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))}-\frac{\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{V}_{(d)}2^{h(N+1)}}\right|\leqslant\frac{\mathscr{V}_{(d)}(k)}{\mathscr{V}_{(d)}}\frac{1}{(\mathscr{W}_{(d)}2^{h}-1)},$$

where

$$\mathscr{W}_{(d)}\coloneqq\frac{\mathscr{V}_{(d)}}{\mathscr{R}_{(d)}}.$$

Then, the following inequality also holds:

$$\begin{aligned}\Sigma_2 &\coloneqq\left|\sum_{k\in\mathbb{N}}\frac{k\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}))}-\sum_{k\in\mathbb{N}}\frac{k\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{V}_{(d)}2^{h(N+1)}}\right|\\ &\leqslant\left|\sum_{k\in\mathbb{N}}\frac{k\mathscr{V}_{(d)}(k)}{\mathscr{V}_{(d)}}\right|\frac{1}{(\mathscr{W}_{(d)}2^{h}-1)}.\end{aligned}$$

From Theorem 21, we conclude

$$\Sigma_2\leqslant\frac{\sqrt{\mathscr{D}_{(d)}}}{\mathscr{W}_{(d)}2^{h}-1}.$$

From Theorem 34 the following inequality also holds for every $k\in\mathbb{N}$, $k\leqslant\mathscr{D}'_{(d)}$:

$$\left|\frac{\mathscr{N}_{\Delta}(S_k,h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}-\frac{\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}\right|\leqslant\frac{\mathfrak{R}_{(d)}2^{hN+1}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}.$$

As $2\mathfrak{R}_{(d)}\geqslant\mathscr{R}_{(d)}$, we conclude

$$\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)\geqslant\mathscr{V}_{(d)}2^{h(N+1)}-\mathfrak{R}_{(d)}2^{hN+1}.$$

Then, we have

$$\left|\frac{\mathscr{N}_{\Delta}(S_k,h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}-\frac{\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}\right|\leqslant\frac{1}{\mathfrak{W}_{(d)}2^{h-1}-1}.$$

As $\mathscr{N}_{\Delta}(S_k,h)=0$, for every $k\in\mathbb{N}$, $k>\mathscr{D}'_{(d)}$, we have

$$\begin{aligned}\Sigma_3 &\coloneqq\left|\sum_{k\in\mathbb{N}}\frac{k\mathscr{N}_{\Delta}(S_k,h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}-\left(\sum_{k\in\mathbb{N}}\frac{k\mathscr{V}_{(d)}(k)2^{h(N+1)}}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)}\right)\right|\\ &\leqslant\sum_{k=0}^{\mathscr{D}'_{(d)}}\frac{k}{\mathfrak{W}_{(d)}2^{h-1}-1}.\end{aligned}$$

Thus, we conclude

$$\Sigma_3 \leqslant \frac{\mathscr{D}'_{(d)}(\mathscr{D}'_{(d)}+1)}{\mathfrak{W}_{(d)}2^h - 2}.$$

The second claim of this lemma follows after noting that

$$\left| \sum_{k\in\mathbb{N}} \frac{k\mathscr{N}_{\Delta}(S_k,h)}{\mathscr{N}_{\Delta}(\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}),h)} - \sqrt{\mathscr{D}_{(d)}} \right| \leqslant \Sigma_1 + \Sigma_2 + \Sigma_3,$$

and noting that $\mathscr{W}_{(d)} \geqslant \mathfrak{W}_{(d)}$. □

Now we are in conditions to prove Theorem 4.

Proof of Theorem 4. First of all, observe that the following equality holds:

$$\mathfrak{W}^{-1}_{(d)} = 2|\det(\Delta)|\zeta(N+1)(D_{(d)}!)^{\frac{N+1}{2}}\left[\frac{T(AD^{Cn}_{(d)}, 2D^{Cn}_{(d)}, N+1)+1}{K_{N+1}} + 1\right]. \tag{32}$$

Now, we recall the following estimates:

- From the definition of Δ in Section 4.1, we have
$$|\det(\Delta)| \leqslant 1.$$

- From the definition of the ζ function, we have
$$\zeta(N+1) \leqslant \zeta(2) \leqslant 2.$$

- From the definition of T in Proposition 10, the following holds:
$$T(AD^{Cn}_{(d)}, 2D^{Cn}_{(d)}, N+1) \leqslant 2D^{Cn}_{(d)}(AD_{(d)} + N + 1)\mathfrak{S}^{(N+1)}.$$

- From the properties of the Γ function and the definitions of $\mathfrak{S}^{(N+1)}$ and K_{N+1}, the following inequalities hold:
$$\frac{\mathfrak{S}^{(N+1)}}{K_{N+1}} \leqslant e^{2/3}(N+1)^{\frac{N+1}{2}}e^{\frac{N+1}{12}} \leqslant [2(N+1)]^{\frac{N+1}{2}}.$$

Now, replacing all these inequalities in Inequality (32), making some elementary calculations and taking logarithms, we obtain

$$\log(\mathfrak{W}^{-1}_{(d)}) \leqslant 2[D_{(d)}(N+1) + Cn]\log D_{(d)} + 2(N+1)\log(N+1) + 20.$$

Finally, for every positive real number $\epsilon > 0$, and for every positive real number h such that

$$h > \log(\mathfrak{W}^{-1}_{(d)}) + 2n\log D_{(d)} - \log\epsilon + 3,$$

The following inequality holds:

$$\frac{(\mathscr{D}'_{(d)})^2 + \sqrt{\mathscr{D}_{(d)}}}{\mathfrak{W}_{(d)} 2^{h-1} - 1} \leqslant \epsilon.$$

Applying Lemma 35 above, the claim of Theorem 4 follows. □

5. Average size of approximate zeros of the projective Newton operator

5.1. Newton's method in projective space

As observed in the introduction, we restrict ourselves to the real case in these pages. The corresponding complex case being quite similar.

The projective Newton's method was introduced in [47]. As in previous pages, we follow the notations of [5].

Let $z \in \mathbb{P}_n(\mathbb{R})$ be a point in the real projective space. The tangent space of $\mathbb{P}_n(\mathbb{R})$ at z is given by the following identity:

$$T_z := \{w \in \mathbb{R}^{n+1} : \langle w, z \rangle = 0\}.$$

Let $(d) := (d_1, \ldots, d_n)$ be a list of degrees and let $F := [f_1, \ldots, f_n] \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be a sequence of homogeneous polynomials. The Jacobian matrix $DF(z)$ defines a linear mapping:

$$DF(z) : \mathbb{R}^{n+1} \to \mathbb{R}^n.$$

We consider the restriction

$$DF(z)|_{T_z} : T_z \to \mathbb{R}^n.$$

When $DF(z)|_{T_z}$ defines a linear isomorphism, we may also consider the inverse mapping:

$$(DF(z)|_{T_z})^{-1} : \mathbb{R}^n \to \mathbb{R}^{n+1}.$$

We finally define the Newton operator of F at z as the mapping:

$$N_F : \mathbb{P}_n(\mathbb{R}) \to \mathbb{P}_n(\mathbb{R})$$

given by the following identity:

$$N_F(\pi(z)) := \pi(z - (DF(z)|_{T_z})^{-1} F(z)),$$

where $\pi : \mathbb{R}^{n+1} \setminus \{0\} \to \mathbb{P}_n(\mathbb{R})$ is the canonical projection and $z \in \mathbb{R}^{n+1} \setminus \{0\}$. Let $L \subseteq \mathbb{P}_n(\mathbb{R})$ be the subset of those $z \in \mathbb{P}_n(\mathbb{R})$ such that $DF(z)|_{T_z}$ is not a linear isomorphism. We obtain the Newton's map:

$$N_F : \mathbb{P}_n(\mathbb{R}) \setminus L \to \mathbb{P}_n(\mathbb{R}).$$

Note that N_F depends only on F as an element of $\mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ and that for $\zeta \notin L$, $N_F(\zeta) = \zeta$ if and only if $F(\zeta) = 0$.

Define a new function $d_T : \mathbb{P}_n(\mathbb{R}) \times \mathbb{P}_n(\mathbb{R}) \to \mathbb{R}$ by

$$d_T(x, y) \coloneqq \tan d_R(x, y),$$

where d_R is the Riemannian distance. The function d_T is not quite a distance function since it does not satisfy the triangle inequality. However it permits the following elegant statement.

Definition 36. We say that $z \in \mathbb{P}_n(\mathbb{R})$ is an approximate zero of $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ with associated actual zero $\zeta \in \mathbb{P}_n(\mathbb{R})$ provided that the points

$$z_0 \coloneqq z,$$

and

$$z_{i+1} \coloneqq N_F(z_i),$$

are defined for all $i \in \mathbb{N}$, $i \geqslant 1$ and such that for every $i \geqslant 1$ the following inequality holds:

$$d_T(\zeta, z_k) \leqslant \left(\frac{1}{2}\right)^{2^k - 1} d_T(\zeta, z).$$

In [49] the quantity $\gamma_0(F, z)$ was defined by the following identity:

$$\gamma_0(F, z) \coloneqq ||\zeta|| \max_{k>1} \left|\left| (DF(\zeta)\,|_{T_\zeta})^{-1} \frac{D^{(k)}F(\zeta)}{k!} \right|\right|^{\frac{1}{k-1}},$$

where $D^{(k)}F(\zeta)$ is the kth derivative of $F : \mathbb{R}^{n+1} \to \mathbb{R}^n$. The following Theorem holds:

Theorem 37 (Shub and Smale [49,50]). *Let $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be a system of homogeneous polynomials equations, and let $\zeta \in \mathbb{P}_n(\mathbb{R})$ such that $F(\zeta) = 0$. Then, for every $z \in \mathbb{P}_n(\mathbb{R})$ the following holds: if*

$$\gamma_0(F, \zeta) d_T(z, \zeta) \leqslant \frac{3 - \sqrt{7}}{2},$$

then z is an approximate zero of F with actual associated zero ζ.

For every $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$, let $\gamma_0(F)$ be the quantity defined by the following identity:

$$\gamma_0(F) \coloneqq \max\{\gamma_0(F, \zeta) : \zeta \in \mathbb{P}_n(\mathbb{R}),\ F(\zeta) = 0\}.$$

Worst-case estimates for the value of $\gamma_0(F)$ can be seen in [11]. Much more interesting than worst-case estimates, average behaviour of $\gamma_0(F)$ was studied in [48]. And for the discrete case, in [12] we introduced sharp estimates for the value of $\gamma_0(F)$ when $F \in \mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ is a polynomial system of equations of bounded bit length. Here, we shall improve the discrete estimates described in Theorem 4 of [12].

Let $F \in \mathscr{H}^{\mathbb{R}}_{(d)}$ be a system of homogeneous polynomial equations and let $\zeta \in \mathbb{P}_n(\mathbb{C})$ be a non-singular projective zero (i.e. $F(\zeta) = 0$ and the Jacobian mapping

$DF(\zeta)|_{T_\zeta} : T_\zeta \to \mathbb{C}^n$ is a non-singular linear mapping). The normalised condition number of system F at ζ is defined by the following identity:

$$\mu_{\text{norm}}(F,\zeta) := ||F||_{\Delta}||DF(\zeta)|^{-1}_{T_\zeta}\,\text{diag}(||\zeta||^{d_i-1}d_i^{\frac{1}{2}})||,$$

where $||F||_{\Delta}$ denotes the norm of F with respect to the Euclidean inner product $\langle\cdot,\cdot\rangle_{\Delta}$ introduced in Section 3.1 above, and $\text{diag}(||\zeta||^{d_i-1}d_i^{\frac{1}{2}})$ is the diagonal matrix given by:

$$\text{diag}(||\zeta||^{d_i-1}d_i^{\frac{1}{2}}) := \begin{pmatrix} ||\zeta||^{d_1-1}d_1^{\frac{1}{2}} & 0 & \cdots & 0 \\ \vdots & \ddots & & \\ 0 & & & ||\zeta||^{d_n-1}d_n^{\frac{1}{2}} \end{pmatrix} \in M_n(\mathbb{R}).$$

We define the normalised condition number $\mu_{\text{norm}}(F)$ as the maximum

$$\mu_{\text{norm}}(F) := \max\{\mu_{\text{norm}}(F,\zeta) : \zeta \in \mathbb{P}_n(\mathbb{C}),\ F(\zeta) = 0\}.$$

In [49], the authors observed that the following inequality holds for every system $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$:

$$\gamma_0(F) \leqslant \frac{D_{(d)}^{\frac{3}{2}}}{2}\,\mu_{\text{norm}}(F).$$

For every positive real number $\varepsilon > 0$, we may also define the tubular neighbourhood $\Sigma(\varepsilon)$ of the discriminant variety $\Sigma \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ in the following terms:

$$\Sigma(\varepsilon) := \{F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)}) : \mu_{\text{norm}}(F) > \varepsilon^{-1}\}.$$

In the proof of Proposition 39 of [12], we proved the following technical statement:

Lemma 38 (Castro et al. [12]). *Let $(d) := (d_1, \ldots, d_n)$ be a list of degrees and assume that*

$$D_{(d)} := \max\{n, d_1, \ldots, d_n\} \geqslant 2.$$

Let $M, s, d \in \mathbb{N}$ be a positive integer numbers given by the following identities:

$$M := 8(n+2)^2, \quad s := 2(n+3)^2, \quad d := 2(D_{(d)}+1).$$

Then, the cone $\widetilde{\Sigma(\varepsilon)} \subseteq \mathscr{H}^{\mathbb{R}}_{(d)}$ over $\Sigma(\varepsilon) \subseteq \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ is a semi-algebraic set. Moreover, $\widetilde{\Sigma(\varepsilon)}$ is the M-projection of an (s,d)-definable semi-algebraic set.

Now, replacing Davenport's estimates by our Proposition 10 above in the arguments of [12] we obtain the following technical improvement:

Theorem 39. *Let $w > 1$ and $h > 0$ be two positive real numbers. Let $\mathscr{N}((d), h)$ be the number of systems of polynomial equations $F \in \mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ of unitarily invariant bit length at most h.*

Let $\mathcal{N}_{\Delta}(w,h)$ be the total number of systems $F\in\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ of unitarily invariant bit length at most h and such that the following inequality holds:

$$\mu_{\mathrm{norm}}(F)\leqslant(w\mathfrak{C}[(d)])^{1/4}, \tag{33}$$

where

$$\mathfrak{C}[(d)]\coloneqq n^3(n+1)N(N-1)\mathscr{D}_{(d)}.$$

Then, if

$$h\geqslant\frac{N}{2}\log N+18(n+2)^2(\log D_{(d)}+\log N)+2(N+1)+\log w, \tag{34}$$

we have

$$\frac{\mathcal{N}_{\Delta}(w,h)}{\mathcal{N}_{\Delta}((d),h)}\geqslant 1-\frac{2}{w}.$$

In particular, given w, h satisfying Inequality (34), *for a randomly chosen system $F\in\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ of unitarily invariant bit length at most h, the following inequality holds with probability at least $1-\frac{2}{w}$:*

$$\gamma_0(F)\leqslant\frac{D_{(d)}^{\frac{3}{2}}}{2}(w\mathfrak{C}[(d)])^{1/4}.$$

Note that we have chosen the uniform probability on finite subsets of $\mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$.

5.2. Average size of approximate zeros of systems of given bit length

Let $d_R:\mathbb{P}_n(\mathbb{R})\times\mathbb{P}_n(\mathbb{R})\to\mathbb{R}$ be the canonical Riemannian distance in the real projective space $\mathbb{P}_n(\mathbb{R})$. Let $d_P:\mathbb{P}_n(\mathbb{R})\times\mathbb{P}_n(\mathbb{R})\to\mathbb{R}$ be the projective distance given by the following identity:

$$d_P(x,y)\coloneqq\sin d_R(x,y).$$

For every projective point $\zeta\in\mathbb{P}_n(\mathbb{R})$ and for every positive real number r, let $B_P(\zeta,r)\subseteq\mathbb{P}_n(\mathbb{R})$ be the closed ball of radius r centred in ζ with respect to the projective distance d_P. Namely,

$$B_P(\zeta,r)\coloneqq\{x\in\mathbb{P}_n(\mathbb{R}):d_P(x,\zeta)\leqslant r\}.$$

The following statement is due to [13]:

Lemma 40. *With the same notations as above,*

$$Vol_{\mathbb{P}}(B_P(\zeta,r))=K_n\int_0^r\frac{x^{n-1}}{\sqrt{1-x^2}}\,dx,$$

where $Vol_{\mathbb{P}}$ is the projective volume discussed in Section 3.

For every $\zeta \in \mathbb{P}_n(\mathbb{R})$ and for every positive real number $r>0$, let $B_T(\zeta, r) \subseteq \mathbb{P}_n(\mathbb{R})$ be the closed ball of radius r centred in ζ with respect to d_T. Namely,

$$B_T(\zeta, r) \coloneqq \{x \in \mathbb{P}_n(\mathbb{R}) : d_T(x, \zeta) \leqslant r\}.$$

Lemma 41. *With the same notations and assumptions as above, the following holds*:

(1) *For every positive real number $r<1$ and for every $\zeta \in \mathbb{P}_n(\mathbb{R})$, the following holds*:

$$B_P(\zeta, r) \subseteq B_T\left(\zeta, \frac{r}{\sqrt{1-r^2}}\right),$$

$$B_P\left(\zeta, \frac{r}{\sqrt{1+r^2}}\right) \subseteq B_T(\zeta, r).$$

(2) *For every positive real number $r<1$ and for every $\zeta \in \mathbb{P}_n(\mathbb{R})$, the following holds*:

$$B_T(\zeta, r) \subseteq B_P(\zeta, r).$$

In particular, we conclude the following estimates for $Vol_{\mathbb{P}}(B_T(\zeta, r))$:

$$Vol_{\mathbb{P}}(B_T(\zeta, r)) \geqslant K_n \int_0^{\frac{r}{\sqrt{1+r^2}}} \frac{x^{n-1}}{\sqrt{1-x^2}}\, dx = K_n \int_0^{\theta} \sin^{n-1}(x)\, dx, \tag{35}$$

where $\tan(\theta) = r$ and

$$Vol_{\mathbb{P}}(B_T(\zeta, r)) \leqslant K_n \int_0^{r} \frac{x^{n-1}}{\sqrt{1-x^2}}\, dx. \tag{36}$$

The obvious arguments would yield:

$$\frac{K_n}{(n-1)} \frac{r^n}{(1+r^2)^{n/2}} \leqslant Vol_{\mathbb{P}}(B_T(\zeta, r)) \leqslant \frac{K_n}{(n-1)} \frac{r^n}{\sqrt{1-r^2}}. \tag{37}$$

Observe that for every $x, y \in \mathbb{R}^{n+1} \backslash \{0\}$, and for every $r>0$, $d_T(\pi(x), \pi(y)) \leqslant r$ if and only if the following inequality holds:

$$||x||^2 ||y||^2 - (1+r^2) |\langle x, y \rangle|^2 \leqslant 0,$$

where $\langle \cdot, \cdot \rangle : \mathbb{R}^{n+1} \times \mathbb{R}^{n+1} \to \mathbb{R}$ is the canonical Euclidean inner product and $||x||^2 \coloneqq \langle x, x \rangle$. Observe that this is a polynomial equation of degree at most 4 in the variables given as the homogeneous coordinates of x and y. In particular, for every $\zeta \in \mathbb{P}_n(\mathbb{R})$ the cone $\widetilde{B_T(\zeta, r)} \subseteq \mathbb{R}^{n+1}$ over $B_T(\zeta, r) \subseteq \mathbb{P}_n(\mathbb{R})$ is a (1,4)-definable semi-algebraic set.

Let $F \in \mathbb{P}(\mathscr{H}^{\mathbb{R}}_{(d)})$ be a system of homogeneous polynomials equations. Let $\zeta \in \mathbb{P}_n(\mathbb{R})$ be a zero (i.e. $\zeta \in V_{\mathbb{R}}(F)$). For every positive number $H>0$, let $\mathscr{N}(\zeta, \eta)$ be the number of points in $\mathbb{P}_n(\mathbb{Q})$ of bit length at most η that satisfy:

$$\gamma_0(F, \zeta) d_T(z, \zeta) \leqslant \frac{3-\sqrt{7}}{2}.$$

With the same notations and assumptions as above, Let $r(F,\zeta)$ be the quantity given by the following identity:

$$r(F,\zeta) \coloneqq \frac{3-\sqrt{7}}{2\gamma_0(F,\zeta)}.$$

Using the notations of Theorem 14, the following equality holds:

$$\mathscr{N}(\zeta,\eta) = \mathscr{N}_I(B_T(\zeta, r(F,\zeta)), \mathbb{Z}^{n+1}, 2^\eta),$$

where I is the identity matrix. Hence, we may also conclude from this Theorem 14 the following statement:

Corollary 42. *With the same notations and assumptions as above, Then, the following inequality holds*:

$$\left|\mathscr{N}(\zeta,\eta) - \frac{Vol_{\mathbb{P}}(B_T(\zeta, r(F,\zeta)))}{(n+1)\zeta(n+1)}\, 2^{\eta(n+1)}\right| \leqslant (\tau + K_{n+1} + 1)2^{\eta n},$$

where $\tau \coloneqq T(1,4,n+1)\mathfrak{S}^{(n+1)} \leqslant 12(n+1)\pi^{\frac{3}{2}n}$.

5.3. Proof of Theorem 5

Theorem 5 immediately follows from the following Proposition:

Proposition 43. *Let* $(d) \coloneqq (d_1, \ldots, d_n)$ *be a list of degrees and let* h, w *be two positive real numbers. Assume that the following inequality holds*:

$$h \geqslant \frac{N}{2}\log N + 18(n+2)^2(\log D_{(d)} + \log N) + 2(N+1) + \log w.$$

Then, for a randomly chosen system $F \in \mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ *of unitarily invariant bit length at most* h, *and for every* $\zeta \in \mathbb{P}_n(\mathbb{R})$ *such that* $\zeta \in V_{\mathbb{R}}(F)$, *there are approximate zeros* $z \in \mathbb{P}_n(\mathbb{Q})$ *of* F *with associated zero* ζ *of bit length at most*

$$\eta > 2(n+2)^2[\log(D_{(d)}+1) + \log(n+1) + 5] + \frac{n}{4}\log(w),$$

with probability at least

$$1 - \frac{2}{w},$$

where

$$D_{(d)} \coloneqq \max\{n, d_1, \ldots, d_n\}.$$

Proof. From Theorem 39, for every system of polynomial equations $F \in \mathbb{P}(\mathscr{H}^{\mathbb{Q}}_{(d)})$ of unitarily invariant bit length at most h, such that h satisfies the following inequality:

$$h \geqslant \frac{N}{2}\log N + 18(n+2)^2(\log D_{(d)} + \log N) + 2(N+1) + \log w,$$

then, the following inequality holds with probability greater than $1-2/w$:

$$\rho_{(d)} \coloneqq \frac{3-\sqrt{7}}{D_{(d)}^{3/2} w^{1/4}(n+1)N^{1/2}\mathscr{D}_{(d)}^{1/4}} \leqslant \frac{3-\sqrt{7}}{2\gamma_0(F,\zeta)} = r(F,\zeta),$$

for every $\zeta \in V_{\mathbb{R}}(F)$.

From Theorem 37 above, for every $F \in \mathbb{P}(\mathscr{H}_{(d)}^{\mathbb{Q}})$ and for every $\zeta \in V_{\mathbb{R}}(F)$, the number of approximate zeros $z \in \mathbb{P}_n(\mathbb{Q})$ of F with associated zero ζ of bit length at most η is greater than

$$\mathscr{N}(\zeta,\eta).$$

From Corollary 42, the following inequality holds:

$$\mathscr{N}(\zeta,\eta) \geqslant \frac{Vol_{\mathbb{P}}(B_T(\zeta, r(F,\zeta)))}{(n+1)\zeta(n+1)} 2^{\eta(n+1)} - (\tau \mathfrak{S}^{(n+1)} + K_{n+1} + 1)2^{\eta n}.$$

Hence, there is at least one approximate zero $z \in \mathbb{P}_n(\mathbb{Q})$ of system F with associated zero ζ of bit length at most η provided that the following inequality holds:

$$\frac{Vol_{\mathbb{P}}(B_T(\zeta, r(F,\zeta)))}{(n+1)\zeta(n+1)} 2^{\eta(n+1)} > (\tau \mathfrak{S}^{(n+1)} + K_{n+1} + 1)2^{\eta n}. \tag{38}$$

As $\rho_{(d)} \leqslant r(F,\zeta)$ with probability greater than $1-2/w$, this inequality holds with probability greater than $1-2/w$, for every $\eta > 0$ such that the following inequality holds:

$$\frac{Vol_{\mathbb{P}}(B_T(\zeta, \rho_{(d)}))}{(n+1)\zeta(n+1)} 2^{\eta(n+1)} > (\tau \mathfrak{S}^{(n+1)} + K_{n+1} + 1)2^{\eta n}. \tag{39}$$

From Inequality (37) we have

$$Vol_{\mathbb{P}}(B_T(\zeta, r(F,\zeta))) \geqslant \frac{K_n}{(n-1)} \frac{r(F,\zeta)^n}{(1+r(F,\zeta)^2)^{n/2}}.$$

Thus, Inequality (39) is satisfied for every $\eta > 0$ such that the following inequality holds:

$$\frac{K_n(\rho_{(d)})^n}{(1+\rho_{(d)}^2)^{n/2}} 2^{\eta} > 2(n^2-1)(\tau + K_{n+1} + 1). \tag{40}$$

This final inequality is satisfied for every $\eta > 0$ such that the following inequality holds:

$$\eta > \left(\frac{n^2}{4} + \frac{3}{2}\right) \log D_{(d)} + \frac{n}{2} \log N + 2(n+3)\log n + \frac{n}{4} \log w.$$

Hence, the claim of this Proposition follows. □

References

[1] B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties, real equation solving, and data structures: the hypersurface case, J. Complexity 13 (1997) 5–27.

[2] B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties and efficient real elimination, Math. Z. 238 (2001) 115–144.

[3] S. Basu, R. Pollack, M.F. Roy, On the combinatorial and algebraic complexity of quantifier elimination, J. ACM 43 (1996) 1002–1045.

[4] R. Benedetti, J.J. Risler, Real Algebraic and Semi-algebraic Sets, Hermann, Paris, 1990.

[5] L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and Real Computation, Springer, New York, 1998.

[6] J. Bochnak, M. Coste, M.-F. Roy, Géométrie Algébrique Réelle, Ergebnisse der Math., 3. Folge, Band 12, Springer, Berlin, 1987.

[7] W.S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors, J. ACM 18 (1971) 478–504.

[8] W.S. Brown, The subresultant PSR algorithm, ACM Trans. Math. Software 4 (1978) 237–249.

[9] W.S. Brown, J.F. Traub, On Euclid's algorithm and the theory of subresultants, J. ACM 18 (1971) 505–514.

[10] D. Castro, M. Giusti, J. Heintz, G. Matera, L.M. Pardo, On the hardness of polynomial equation solving, Found. Comput. Math (2003), submitted.

[11] D. Castro, K. Hägele, J.E. Morais, L.M. Pardo, Kronecker's and Newton's approaches to solving: a first comparison, J. Complexity 17 (2001) 212–303.

[12] D. Castro, J.L. Montaña, L.M. Pardo, J. San Martín, The distribution of condition numbers of rational data of bounded bit length, Found. Comput. Math. 1 (1) (2002) 1–52.

[13] K.K.S. Choi, On the distribution of points in projective space of bounded height, Trans. Amer. Math. Soc. 352 (2000) 1071–1111.

[14] G.E. Collins, Subresultants and reduced polynomial remainder sequence, J. ACM 14 (1967) 128–142.

[15] H. Davenport, On a principle of Lipschitz, J. London Math. Soc. 26 (1951) 179–183.

[16] P. Erdös, P. Turán, On a problem in the theory of uniform distribution. I, Indagagtiones. Math. 10 (1948) 370–378.

[17] P. Erdös, P. Turán, On a problem in the theory of uniform distribution. II, Indag. Math. 10 (1948) 406–413.

[18] M. Giusti, J. Heintz, La Détermination des Points Isolés et de la Dimension d'une Varieté Algébrique Peut se Faire en Temps Polynomial, in: D. Eisenbud, L. Robbiano (Eds.), Computational Algebraic Geometry and Commutative Algebra, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, Symposia Matematica, Vol. XXXIV, Cambridge University Press, Cambridge, 1993, pp. 216–256.

[19] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, L.M. Pardo, Lower bounds for diophantine approximations, J. Pure Appl. Algebra 117 & 118 (1997) 277–317.

[20] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, When polynomial equation systems can be "Solved" fast?, in: G. Cohen, M. Giusti, T. Mora (Eds.), Proceedings of the 11th International Symposium Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris, Lecture Notes in Computer Science, Vol. 948, Springer, Berlin, 1995, pp. 205–231.

[21] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, Le Rôle des Structures de Données dans les Problèmes d'Élimination, C. R. Acad. Sci. Paris Série I 325 (1997) 1223–1228.

[22] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, J. Pure Appl. Algebra 124 (1998) 101–146.

[23] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (2001) 154–211.

[24] W. Habicht, Eine Verallgemeirung des Sturmschen Wurzelzählverfahrens, Comment. Math. Helv. 21 (1948) 99–116.

[25] K. Hägele, J.E. Morais, L.M. Pardo, M. Sombra, On the intrinsic complexity of the arithmetic nullstellensatz, J. Pure Appl. Algebra 146 (2) (2000) 103–183.

[26] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 1938.
[27] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theor. Comput. Sci. 24 (1983) 239–277.
[28] J. Heintz, G. Matera, Luis M. Pardo, R. Wachenchauzer, The intrinsic complexity of parametric elimination methods, Electron. J. SADIO 1 (1) (1998) 37–51.
[29] J. Heintz, G. Matera, A. Waissbein, On the time–space complexity of geometric elimination procedures, Appl. Algebra Eng. Commun. Comput. 11 (2001) 239–296.
[30] J. Heintz, C.P. Schnorr, Testing polynomials which are easy to compute, in: Logic and Algorithmic (an International Symposium in Honour of Ernst Specker), Monographie n. 30 de l'Enseignement Mathématique, 1982, pp. 237–254 (A preliminary version appeared in Proceedings of the 12th Annual ACM Symposium on Computing, 1980, pp. 262–268).
[31] P. Koiran, Approximating the volume of definable sets, in: 36th Annual IEEE Symposium FOCS, 1995, pp. 134–141.
[32] T. Krick, L.M. Pardo, A computational method for diophantine approximation, in: Algorithms in Algebraic Geometry and Applications, Proceedings MEGA'94, Progress in Mathematics, Vol. 143, Birkhäuser, Basel, 1996, pp. 193–254.
[33] T. Krick, Luis M. Pardo, M. Sombra, Sharp estimates for the arithmetic nullstellensatz, Duke Math. J. 109 (2001) 521–598.
[34] G. Lecerf, Une Alternative aux Méthodes de Réécriture pour la Résolution des Systèmes Algébriques, Ph.D. Thesis, École Polytechnique, France, 2001.
[35] T. Lickteig, M.F. Roy, Sylvester–Habicht sequences and fast cauchy index computation, J. Symb. Comput. 31 (2001) 315–341.
[36] S. Lojasiewicz, Ensembles Semi-Analytiques, Lecture Notes, Institut des Hautes Etudes Scientiques, Presses Universitaires de France, 1966.
[37] R. Loos, Generalised polynomial remainder sequences, in: B. Buchberger, G.E. Collins, R. Loos, R. Albrecht (Eds.), Computer Algebra, Symbolic and Algebraic Computation, Springer, Berlin, 1982.
[38] J. Milnor, On the Betti numbers of real varieties, Proc. Amer. Math. Soc. 15 (1964) 275–280.
[39] J.L. Montaña, L.M. Pardo, Lower bounds for arithmetic networks, Appl. Algebra Eng. Commun. Comput. 4 (1993) 1–24.
[40] L.J. Mordell, On some arithmetical results in the geometry of numbers, Compositio Math. 1 (1934) 248–253.
[41] O.A. Oleinik, Estimates of the Betti numbers of real algebraic hypersurfaces, Mat. Sbornik 70 (1951) 635–640.
[42] O.A. Oleinik, I.B. Petrovsky, On the topology of real algebraic surfaces, Izv. Akad. Nauk SSSR (in Trans. of the Amer. Math. Soc.) 1 (1962) 399–417.
[43] L.M. Pardo, How lower and upper complexity bounds meet in elimination theory, in: G. Cohen, M. Giusti, T. Mora (Eds.), Proceedings of the 11th International Symposium Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris, Lecture Notes in Computer Science, Vol. 948, Springer, Berlin, 1995, pp. 33–69.
[44] L.M. Pardo, Universal elimination requires exponential running time (Extended Abstract), in: A. Montes (Ed.), Proceedings EACA' 2000, Barcelona, 2000, pp. 25–51.
[45] M.F. Roy, Basic algorithms in real algebraic geometry and their complexity: from Sturm's theorem to the existential theory of reals, in: F. Broglia (Ed.), Lecture on Real Algebraic Geometry in Memoriam of Mario Raimondo, de Gruyter Expositions in Mathematics, Vol. 23, Walter de Gruyter and Co. 1996, pp. 1–67.
[46] A. Seidenberg, A new decision method for elementary algebra, Ann. Math. 60 (2) (1954) 365–374.
[47] M. Shub, Some remark's on Bézout's theorem and complexity theory, in: M. Hirsch, J. Marsden, M. Shub (Eds.), From Topology to Computation: Proceedings of the Smalefest, Springer, 1993, pp. 443–455.
[48] M. Shub, S. Smale, Complexity of Bézout's theorem II: volumes and probabilities, in: Proceedings MEGA' 92, Progress in Mathematics, Vol. 109, Birkhäuser, Basel, 1993, pp. 267–285.

[49] M. Shub, S. Smale, Complexity of Bézout's theorem I: geometric aspects, J. Amer. Math. Soc. 6 (1993) 459–501.
[50] M. Shub, S. Smale, Complexity of Bezout's theorem. IV: probability of success; extensions, SIAM J. Numer. Anal. 33 (1996) 128–148.
[51] A. Tarski, A Decision Method for Elementary Algebra and Geometry, RAND Corporation, Santa Monica, CA, 1948.
[52] R. Thom, Sur l'Homologie des Variétés Algébriques Réelles, in: Differential and Combinatorial Topology, A Symposium in Honor of Marston Morse, Princeton University Press, Princeton, 1965, pp. 255–265.
[53] J.D. Vaaler, Some extremal functions in Fourier analysis, Bull. Amer. Math. Soc. (NS) 12 (1985) 183–216.
[54] H.E. Warren, Lower bounds for approximation by non linear manifolds, Trans. AMS 133 (1968) 167–178.
[55] H. Weyl, Über die Gleichverteilung von Zahlen Modulo 1, Math. Ann. 77 (1916) 313–352.